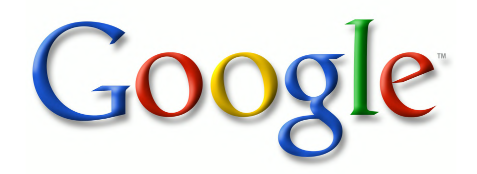
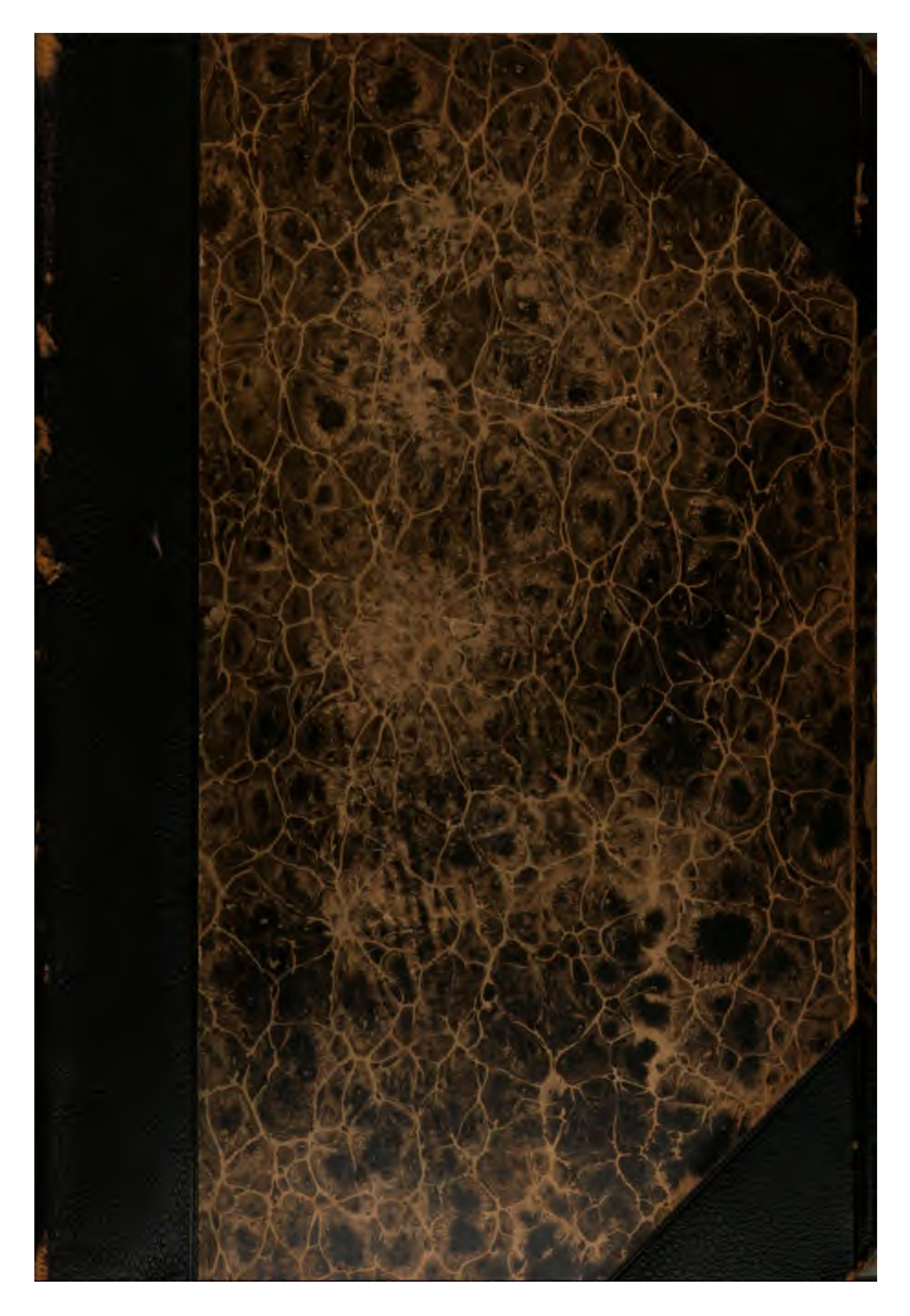




ZAHLENTHEORIE

VERSUCH
EINER
GESAMTDARSTELLUNG DIESER WISSENSCHAFT
IN IHREN HAUPTTEILEN

VON

PAUL BACHMANN

FÜNFTER TEIL
ALLGEMEINE ARITHMETIK DER ZAHLENKÖRPER



LEIPZIG
DRUCK UND VERLAG VON B. G. TEUBNER
1905

ALLGEMEINE ARITHMETIK DER ZAHLENKÖRPER

DARGESTELLT

VON

PAUL BACHMANN

LEIPZIG
DRUCK UND VERLAG VON B. G. TEUBNER
1905

RICHARD DEDEKIND

IN

DANKBARKEIT UND VEREHRUNG

GEWIDMET

Vorrede.

In Fortführung meiner Gesamtdarstellung der Zahlentheorie übergebe ich hiermit den fünften Teil derselben, welcher die Theorie der algebraischen Zahlen zum Gegenstande hat, dem Leser, wohl entgegen seiner Erwartung, da er berechtigt wäre, zunächst meine Arithmetik der quadratischen Formen beendet zu sehen. Aber zu mancherlei Gründen, die mich an der Ausarbeitung des zweiten Teiles der letzteren noch immer behindert, gesellte sich der Wunsch, dasjenige Gebiet der Zahlentheorie, welches als ihre höchste bisher erreichte Spitze und zugleich als ihr eigentlicher Grundstock bezeichnet werden darf und welches mit Rücksicht auf die moderne zahlentheoretische Forschung das aktuellste Interesse darbietet, möglichst bald einem größeren Leserkreise in leicht verständlicher Darstellung zugänglich zu machen. So entschloß ich mich, zunächst wenigstens die allgemeine Arithmetik der Zahlenkörper zu veröffentlichen, diejenige spezieller Zahlenkörper einem späteren Bande vorbehaltend.

Die Geschichte dieser Disziplin geht auf Gauß zurück, der mit seiner „Erweiterung des Feldes der Arithmetik" durch Einführung der komplexen ganzen Zahlen von der Form $a + b\sqrt{-1}$ den Grund zu ihr legte. In der Folge namentlich durch Kummer weiter entwickelt und durch dessen geniale Schöpfung der idealen Zahlen zu voller Entfaltung erst eigentlich befruchtet, erhielt sie ihre allgemeine Ausgestaltung vornehmlich durch zwei Forscher, R. Dedekind und L. Kronecker, die ganz unabhängig voneinander und auf den verschiedensten Wegen dies Ziel erreichten. Der Erstere hat teils in einem Supplemente zu den von ihm herausgegebenen Dirichletschen

Vorlesungen über Zahlentheorie, teils in einer Reihe besonderer Arbeiten seine Theorie der algebraischen Zahlen mit gleich bewundernswertem Scharfsinn wie systematischem Aufbau entwickelt, Kronecker die seinige leider nur in einer lückenhaften Skizzierung ihrer Grundzüge*) in der „Festschrift zu Herrn E. E. Kummers Doktor-Jubiläum 10. Sept. 1881“, gleichwohl aber mit einer großartigen Erfassung des gesamten Gebietes der algebraischen Größen und somit weit über Dedekinds Betrachtungen hinausgehend, obwohl auch diese (s. seine gemeinsam mit Weber veröffentlichte Arbeit über algebraische Funktionen**)) weiterer Ausdehnung fähig sind. Ursprünglich war es meine Absicht, in meinem Werk eine Art synoptischer Darstellung der Theorieen dieser beiden Forscher zu versuchen, sie, wo sie nicht zu verschmelzen sind, doch vergleichend nebeneinander zu stellen.***) Wenn ich nun hiervon abstand und, zwischen beiden Theorieen wählend, mich prinzipiell für diejenige Dedekinds entschied, so bestimmte mich dazu der Gedanke, daß es für mein an sich schon so umfängliches Werk geraten sei, die Grenzen der reinen Zahlentheorie womöglich nicht zu überschreiten. Bei der aus dieser Erwägung folgenden Beschränkung auf die algebraischen Zahlen erschien es dann aber mir sachgemäßer, Dedekinds rein arithmetischen Gesichtspunkten, so weit sie reichen, zu folgen; dünkt mich doch in der Tat alsdann sein wissenschaftlicher Standpunkt korrekt, auf welchem ihm „das methodische Hilfsmittel der unbestimmten Koeffizienten“ und „die Einmischung der Funktionen von Variabeln ein der Sache fremdes Hilfsmittel erscheint“, mit dem er sich nicht befreunden

*) Neuerdings hat J. König in seiner Einleitung in die allgemeine Theorie der algebraischen Größen (aus dem Ungarischen übertragen vom Verfasser) Lpzg. 1903 eine Bearbeitung der Kroneckerschen Theorie veröffentlicht und damit einem schon von Dedekind (in der Vorrede zur 4. Auflage von Dirichlets Vorlesungen über Zahlentheorie) geäußerten Wunsche in sehr gründlicher Weise entsprochen.

**) Theorie der algebraischen Funktionen einer Veränderlichen, im Journal f. d. r. u. a. Math. 92, p. 181.

***) Eine sehr glückliche Vermittlung zwischen beiden Theorieen gab H. Weber in seinem Lehrbuch der Algebra, 2. Aufl., 1898/99, 2. Bd., 4. Buch.

könne, während die rein arithmetischen Grundvorstellungen Dedekinds, die Moduln, die Ideale, so abstrakt sie sind, gleichwohl, auf die einfachste Weise aus ganzen Zahlen des betrachteten Körpers gebildet, wahrhaft ursprünglichen Charakter an sich tragen und ihn in der Theorie erweisen. Indem ich so im Aufbau meines Werkes vorzüglich auf Dedekinds Forschungen gefußt habe, war ich doch, um mit seinen Resultaten auch diejenigen anderer Forscher verschmelzen zu können, die teilweise über jene hinausgehen und mit den Hilfsmitteln Dedekinds nicht oder doch nur viel umständlicher erreicht werden können, genötigt, in geringem Umfange auch Kroneckersche Gesichtspunkte zu berühren und jenes Hilfsmittel der unbestimmten Koeffizienten heranzuziehen. Zur ersteren Kategorie zählt der Henselsche Nachweis von der allgemeinen Verwendbarkeit der höheren Kongruenzen zur Zerlegung der reellen ganzen Zahlen in Primidealfaktoren; hier bedarf es, um „den Gesetzen der Teilbarkeit wiederum Raum zur vollen Wirksamkeit zu schaffen"*), nämlich um die formale Gleichmäßigkeit der Zerlegung in allen Fällen zu sichern, notwendig der „Assoziation der Unbestimmten" durch die Benutzung der Fundamentalform. Zur zweiten Kategorie rechnen u. a. Dedekinds Sätze über die Teiler der Diskriminante, welche Hensel nach Kronecker sehr viel einfacher aus seiner Theorie der Fundamentalgleichung gewann. Doch ist eben hier jenes Kroneckersche Hilfsmittel nur ein bequemes, nicht aber erforderliches, wie denn jene Sätze durch Hensel von seiner neuesten Auffassung der Theorie der algebraischen Zahlen aus durch einen noch präziser gefaßten ersetzt worden sind. Von dieser Henselschen Theorie soll anhangsweise dem Leser wenigstens noch soviel mitgeteilt werden, als notwendig ist, um diese genauere Fassung zu erläutern und zu begründen.

Große Förderung bei der Ausarbeitung meines Werks verdanke ich dem vortrefflichen Berichte Hilberts über „die Theorie der algebraischen Zahlkörper" im Jahresberichte der Deutschen Mathematiker-Vereinigung v. J. 1894/95; insbeson-

*) Kronecker, Festschrift, p. 48.

dere habe ich denselben dem Schlußkapitel über den Galoisschen Zahlenkörper in wesentlichen Teilen zugrunde gelegt. Dieser Körper, obwohl er schon ein Körper speziellen Charakters ist und sonach der vorbehaltenen Fortsetzung dieses Werkes zuzuweisen sein sollte, mußte hier schon zur Betrachtung kommen kraft seiner eigentümlichen Stellung, nach der er andererseits wieder als jeden beliebigen Körper in sich enthaltend angesehen werden kann; so bildet das ihn behandelnde Kapitel zugleich den Abschluß des gegenwärtigen und den Übergang zu dem geplanten zukünftigen Werke, dem ich auch die Hilbertschen Untersuchungen über relativ-zyklische und andere Körper trotz ihres allgemeineren Charakters als solche über spezielle Körper zuweise.

Möchte es mir gelungen sein, die Arithmetik der Zahlenkörper, von der mit ebenso schönen wie zutreffenden Worten Dedekind rühmt, daß die Erkenntnis, die sie liefert, zu sehen, wie die ganze Mannigfaltigkeit aller möglichen Zahlenkörper von eben denselben, allgemeingültigen einfachen Gesetzen beherrscht werde, wie die gewöhnlichen ganzen Zahlen, einen hohen Grad nicht nur theoretischen, sondern geradezu ästhetischen Interesses gewähre*) — möchte es mir gelungen sein, sie klar und leicht faßlich zu gestalten und so recht Vielen den Genuß jener Erkenntnis zu vermitteln. Vielleicht daß ich den rechten Weg traf, „ohne der Systematik etwas zu vergeben, eine gemischte Methode als historisches, heuristisches und vergleichendes Prinzip mit gutem Erfolge zur Anwendung zu bringen.“**)

Weimar, den 21. Juli 1904.

*) Dedekind, sur la théorie des nombres entiers algébriques, Paris 1877, p. 104.

**) F. Meyer, Ztschr. f. Math. u. Physik 1895, histor.-liter. Abt. p. 91.

Inhaltsverzeichnis.

Erstes Kapitel.

Die Zahlenkörper.

Zweites Kapitel.

Die Moduln.

Drittes Kapitel.

Divisorensysteme. Höhere Kongruenzen.

Viertes Kapitel.

Die ganzen algebraischen Zahlen.

Seite

Fünftes Kapitel.

Die Entwicklung der Theorie am Beispiel des quadratischen Körpers erläutert.

Sechstes Kapitel.

Die Arithmetik der Körperideale.

Siebentes Kapitel.

Von den Diskriminantenteilern.

Achtes Kapitel.

Von den Einheiten.

Neuntes Kapitel.
Ideale einer Ordnung und die Anzahl ihrer Klassen.

Seite

Zehntes Kapitel.

Die zerlegbaren Formen.

Elftes Kapitel.

Unterkörper und Oberkörper.

Zwölftes Kapitel.

Der Galoissche Körper.

Anhang.

Reihenentwicklung der Zahlen.

Erstes Kapitel.

Die Zahlenkörper.

1. Die Grundlage jeder Rechnung ist die Reihe der natürlichen, d. i. der positiven ganzen Zahlen, denen jedoch schon, um in allen Fällen die Subtraktion zu ermöglichen, die Null und die negativen ganzen Zahlen hinzuzufügen sind. Weiter aber nötigen bereits die einfachsten Probleme, nämlich die Auflösung von Gleichungen ersten Grades dazu, auch die gebrochenen Zahlen in die Rechnung zuzulassen, welche dann zusammen mit den ganzen das Gebiet der rationalen Zahlen ausmachen. Doch auch diese reichen für die höheren Bedürfnisse der Rechnung nicht aus. Vielmehr führt die Auflösung der Gleichung zweiten Grades mit beliebigen rationalen Koeffizienten, d. i. der Gleichung

$$ax^2 + bx + c = 0$$

mittels der Formel

$$x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

wieder zwei neue Gattungen von Zahlen herbei, so oft die Zahl $d = b^2 - 4ac$ keine Quadratzahl ist. Wenn nämlich in dieser Voraussetzung d positiv ist, so ist der Ausdruck $\sqrt{d}$ keiner rationalen Zahl gleich also irrational, und kann dann arithmetisch vermittels des Grenzbegriffs, etwa als gemeinsamer Grenzwert zweier unbegrenzter, gegen einander konvergierender Reihen rationaler Werte erfaßt werden; derselbe Grenzbegriff ermöglicht ferner die Feststellung des Gebietes der reellen Werte, welches die sämtlichen rationalen und irrationalen Zahlen umschließt. Ist dagegen $d = -\delta$ eine negative Zahl, so findet sich nicht einmal in diesem erweiterten Zahlengebiete eine der Quadratwurzel aus d gleiche Zahl, da ihm viel-

mehr nur $\sqrt{\delta}$ angehört, und man findet $\sqrt{d} = i \cdot \sqrt{\delta}$, wo $i = \sqrt{-1}$ die sogenannte imaginäre Einheit ist, und wird auf solche Weise in das Gebiet der imaginären und noch allgemeiner in dasjenige der komplexen Zahlen geführt, welche, aus einem reellen und einem imaginären Bestandteile zusammengesetzt, von der Form $\alpha + \beta i$ sind. Daß hierbei dem Zeichen $\sqrt{-1}$ eine reale, anschauliche Bedeutung beigelegt werden kann, hat zuerst Gauß in genialer Weise erkannt; aber auch ein rein arithmetischer Sinn läßt sich mit ihm verbinden, indem man jede Beziehung zwischen komplexen Zahlen als eine Kongruenz auffassen darf, die aus ihr hervorgeht, wenn man darin $\sqrt{-1}$ durch eine Unbestimmte u ersetzt und $u^2 + 1$ zum Modulus wählt (Kronecker).

Geht man nun weiter zu den allgemeinen Gleichungen dritten und vierten Grades mit rationalen Koeffizienten, deren algebraische Auflösbarkeit Cardano und Ferrari gelehrt haben, so geben deren Wurzelausdrücke keinen Anlaß zur Einführung neuer Zahlengattungen. Auch die Wurzeln binomischer Gleichungen beliebiger Grade, insonderheit die Wurzeln der Gleichung $x^n = 1$, nämlich die Werte

$$x = \cos\frac{2\varkappa\pi}{n} + i\sin\frac{2\varkappa\pi}{n}$$
$$(\text{für } \varkappa = 0, 1, 2, \cdots, n-1),$$

gehören dem Gebiete der komplexen Zahlen an. Die nicht binomischen Gleichungen höheren als des vierten Grades, d. h. die Gleichungen von der Form

$$(1) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0,$$
$$(n > 4),$$

wo der Koeffizient des höchsten Gliedes stets als Eins gedacht werden darf und soll, während für die übrigen beliebige rationale Werte vorausgesetzt werden, sind zwar, wie Abel gezeigt hat, nicht mehr immer algebraisch auflösbar; aber wir verdanken wieder Gauß den ersten strengen Nachweis der Tatsache, daß auch eine jede solche Gleichung im Gebiete der komplexen Zahlen eine Wurzel besitzt und daß somit die ganze Funktion, welche ihre linke Seite bildet, in n Linearfaktoren zerfällt werden kann:

(2) $x^n + a_1 x^{n-1} + \cdots + a_n = (x-\alpha)(x-\alpha^{(1)}) \cdots (x-\alpha^{(n-1)})$,

während $\alpha, \alpha', \cdots \alpha^{(n-1)}$ endliche komplexe Zahlen bedeuten. Aus solcher Identität ergeben sich unmittelbar die Beziehungen:

$$(3) \quad \begin{cases} \alpha + \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n-1)} = -a_1, \\ \alpha\alpha^{(1)} + \alpha\alpha^{(2)} + \cdots + \alpha^{(n-2)}\alpha^{(n-1)} = +a_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha\alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n-1)} = (-1)^n a_n, \end{cases}$$

nach denen die einfachsten symmetrischen ganzen Funktionen von den Wurzeln der Gleichung (1) den mit passenden Vorzeichen genommenen Koeffizienten der letzteren gleich sind.

Dieser Gaußsche Fundamentalsatz[1]) bildet — neben den elementarsten Sätzen der Determinantentheorie — die einzige aber auch unentbehrliche algebraische Grundlage der folgenden Betrachtungen, insofern erst durch ihn deren reale Bedeutung, nämlich die Existenz der Größen, deren Theorie wir zu entwickeln unternehmen, gewährleistet wird.

Wir bezeichnen nämlich jetzt jede Wurzel einer Gleichung beliebigen Grades n von der Form (1) mit rationalen Koeffizienten als eine algebraische Zahl, und werden die Eigenschaften der so definierten Zahlen untersuchen. Sind insbesondere die Koeffizienten der Gleichung ganze Zahlen, so werden die durch sie definierten algebraischen Zahlen auch ganze algebraische Zahlen, oder, wo kein Mißverständnis zu befürchten ist, kurz ganze Zahlen genannt werden; bei solcher abgekürzten Bezeichnung sind dann aber die gewöhnlichen ganzen Zahlen, welche die einfachste Art jener Zahlen bilden, zum Unterschiede deutlicher als rationale ganze Zahlen zu kennzeichnen.

2. Das Erste, was hier festgestellt werden soll, ist der folgende Satz:

Sind α, β zwei (identische oder verschiedene) algebraische Zahlen, so sind auch $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$, $\frac{\alpha}{\beta}$, d. i. Summe, Differenz, Produkt und Quotient derselben, falls in letzterem der Nenner von Null ver-

1) Der übrigens auch für beliebige komplexe a_i gilt.

schieden ist, algebraische Zahlen.[1]) In der Tat, sind α, β als Wurzeln der beiden Gleichungen

$$(4) \qquad \begin{cases} x^m + A_1 x^{m-1} + A_2 x^{m-2} + \cdots + A_m = 0 \\ x^n + B_1 x^{n-1} + B_2 x^{n-2} + \cdots + B_n = 0 \end{cases}$$

resp., deren Koeffizienten rationale Zahlen sind, bestimmt, so setze man $mn = p$ und bezeichne mit $\omega_1, \omega_2, \cdots, \omega_p$ die p Produkte $\alpha^\mu \beta^\nu$, welche den Exponenten

$$\mu = 0, 1, 2, \cdots, m-1; \quad \nu = 0, 1, 2, \cdots, n-1$$

entsprechen. Dann läßt sich, wenn unter ω zunächst eine der Zahlen $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ verstanden wird, jedes der Produkte $\omega\omega_1$, $\omega\omega_2$, $\cdots$, $\omega\omega_p$, wie leicht zu übersehen ist, in der Form

$$(5) \qquad h_1 \omega_1 + h_2 \omega_2 + \cdots + h_p \omega_p$$

mit rationalen Koeffizienten h_i darstellen. Um dies z. B. für $\omega = \alpha + \beta$ zu erkennen, bemerke man zunächst die Gleichung

$$(6) \qquad (\alpha + \beta) \cdot \alpha^\mu \beta^\nu = \alpha^{\mu+1} \beta^\nu + \alpha^\mu \beta^{\nu+1}.$$

Wäre hier $\mu < m - 1$, $\nu < n - 1$, so gehörten beide Summanden der Reihe $\omega_1, \omega_2, \cdots, \omega_p$ an, und die Form (5) wäre bestätigt. Wäre $\mu = m - 1$, $\nu < n - 1$, so ließe sich der erste Summande mittels der Identität

$$\alpha^m + A_1 \alpha^{m-1} + \cdots + A_m = 0$$

durch

$$-A_1 \alpha^{m-1} \beta^\nu - A_2 \alpha^{m-2} \beta^\nu - \cdots - A_m \alpha^0 \beta^\nu$$

ersetzen und man käme wieder auf die Form (5) zurück. Wäre im Gegenteil $\mu < m - 1$, $\nu = n - 1$, so gelänge das Gleiche mit Hilfe der Identität

$$\beta^n + B_1 \beta^{n-1} + \cdots + B_n = 0;$$

und, wenn endlich zugleich $\mu = m - 1$, $\nu = n - 1$ wäre, so hätte man offenbar zu demselben Zwecke nur beide Identitäten in Anspruch zu nehmen. Was aber so für $\alpha + \beta$ bewiesen, gilt

---

1) Die von Dedekind herrührenden Beweise der Sätze in dieser und in der folgenden Nummer findet man bereits in des Verfassers „Vorlesungen über die Natur der Irrationalzahlen", Kap. 2; wegen der grundlegenden Bedeutung der Sätze sind sie hier reproduziert.

ersichtlich gleichermaßen auch für $\alpha - \beta$ und $\alpha \cdot \beta$; und somit kann man in allen drei Fällen p Gleichungen aufstellen:

$$(7)\qquad \begin{cases} \omega\omega_1 = h_1'\omega_1 + h_2'\omega_2 + \cdots + h_p'\omega_p, \\ \omega\omega_2 = h_1''\omega_1 + h_2''\omega_2 + \cdots + h_p''\omega_p, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \omega\omega_p = h_1^{(p)}\omega_1 + h_2^{(p)}\omega_2 + \cdots + h_p^{(p)}\omega_p, \end{cases}$$

in denen die Koeffizienten rationale Zahlen sind. Gibt man diesen aber die Gestalt:

$$(8)\qquad \begin{cases} 0 = (h_1' - \omega)\,\omega_1 + h_2'\omega_2 + \cdots + h_p'\omega_p, \\ 0 = h_1''\omega_1 + (h_2'' - \omega)\,\omega_2 + \cdots + h_p''\omega_p, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0 = h_1^{(p)}\omega_1 + h_2^{(p)}\omega_2 + \cdots + (h_p^{(p)} - \omega)\,\omega_p \end{cases}$$

und bedenkt, daß unter den Zahlen $\omega_1, \omega_2, \cdots \omega_p$ auch die von Null verschiedene Zahl $\alpha^0\beta^0 = 1$ vorkommt, so schließt man daraus notwendig das Verschwinden ihrer Determinante:

$$(9)\qquad \begin{vmatrix} h_1' - \omega, & h_2', & \cdots\cdots, & h_p' \\ h_1'', & h_2'' - \omega, & \cdot\cdot, & h_p'' \\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\ h_1^{(p)}, & h_2^{(p)}, & \cdots\cdots, & h_p^{(p)} - \omega \end{vmatrix} = 0,$$

eine Gleichung, der man durch Entwicklung nach den Potenzen von ω die Gestalt

$$(10)\qquad \omega^p + H_1\omega^{p-1} + H_2\omega^{p-2} + \cdots + H_p = 0$$

geben kann, wo die Koeffizienten H_i als ganze, ganzzahlige Funktionen der rationalen Zahlen $h_k^{(i)}$ selbst rationale Zahlen sein werden. Somit ist ω eine algebraische Zahl.

Es sei hier sofort hervorgehoben, daß zugleich mit den Koeffizienten A_i, B_i offenbar auch die Koeffizienten $h_k^{(i)}$, also endlich auch die Koeffizienten H_i rationale ganze Zahlen sein werden; aus dieser Bemerkung aber ergibt sich der überaus wichtige Zusatz: die Summe, die Differenz und das Produkt von zwei *ganzen* algebraischen Zahlen ist stets wieder eine *ganze* algebraische Zahl.

Ist nun ferner die algebraische Zahl β von Null verschieden, so darf auch das Gleiche vom Koeffizienten B_n angenommen werden, da sonst β Wurzel einer Gleichung geringeren Grades als

n sein würde, die dann statt der Gleichung n^{ten} Grades der Betrachtung zu Grunde gelegt werden könnte. Da somit die β bestimmende Gleichung sich schreiben läßt, wie folgt:

$$\left(\frac{1}{\beta}\right)^n + \frac{B_{n-1}}{B_n}\cdot\left(\frac{1}{\beta}\right)^{n-1} + \cdots + \frac{B_1}{B_n}\cdot\frac{1}{\beta} + \frac{1}{B_n} = 0,$$

so ist $\frac{1}{\beta}$ als Wurzel der Gleichung

$$x^n + \frac{B_{n-1}}{B_n}\cdot x^{n-1} + \cdots + \frac{B_1}{B_n}\cdot x + \frac{1}{B_n} = 0$$

mit rationalen Koeffizienten, zugleich aber auch nach dem bereits Bewiesenen $\frac{\alpha}{\beta}$ eine algebraische Zahl.

Der auf solche Weise bewiesene Satz kann folgendermaßen verallgemeinert werden: Jede rationale Funktion einer oder mehrerer algebraischer Zahlen mit ganzzahligen Koeffizienten, d. i. jeder aus einer oder mehreren algebraischen Zahlen und ganzen Zahlen auf rationale Weise gebildete Ausdruck ist wieder eine algebraische Zahl; denn jeder Ausdruck dieser Art entsteht aus den gegebenen algebraischen Zahlen durch eine endliche Folge der betrachteten vier Grundoperationen.

Insbesondere gilt hier wieder der wichtige Zusatz, welcher den früheren verallgemeinert:

Jede *ganze* ganzzahlige Funktion von einer oder mehreren *ganzen* algebraischen Zahlen ist auch eine solche Zahl.

3. Es besteht ein noch allgemeinerer Satz, der sich ganz auf die gleiche Weise begründen läßt. Ist nämlich ω Wurzel einer algebraischen Gleichung, deren Koeffizienten algebraische Zahlen sind, so ist ω selbst eine algebraische Zahl.

In der Tat, bestehen zugleich mit der Gleichung

$$\omega^n + \alpha\omega^{n-1} + \beta\omega^{n-2} + \cdots + \gamma = 0$$

die folgenden Identitäten:

$$\begin{aligned} \alpha^a + A_1\alpha^{a-1} + \cdots + A_a &= 0 \\ \beta^b + B_1\beta^{b-1} + \cdots + B_b &= 0 \\ \cdots\cdots\cdots&\cdots \\ \gamma^c + C_1\gamma^{c-1} + \cdots + C_c &= 0, \end{aligned}$$

in denen die Koeffizienten rationale Zahlen sind, und bezeichnet man jetzt mit p das Produkt $nab\cdots c$, mit $\omega_1, \omega_2, \cdots, \omega_p$ aber die sämtlichen Produkte

$$\omega^{n'}\alpha^{a'}\beta^{b'}\cdots\gamma^{c'}$$

für

$$\begin{aligned} n' &= 0,\ 1,\ 2, \cdots, n-1, \\ a' &= 0,\ 1,\ 2, \cdots, a-1, \\ b' &= 0,\ 1,\ 2, \cdots, b-1, \\ &\ldots\ldots\ldots \\ c' &= 0,\ 1,\ 2, \cdots, c-1, \end{aligned}$$

so überzeugt man sich genau, wie bei dem vorigen Beweise, daß durch bloße Verwendung jener Identitäten jedes der Produkte $\omega\omega_1, \omega\omega_2, \cdots, \omega\omega_p$ auf die Form

$$h_1\omega_1 + h_2\omega_2 + \cdots + h_p\omega_p$$

gebracht werden kann, in welcher die Koeffizienten h_i aus den $A_i, B_i, \cdots, C_i$ nur durch Additionen, Subtraktionen und Multiplikationen entstehen, also rational sind. So erhält man wieder p Gleichungen von der Form (7) und aus ihnen zuletzt eine Gleichung von der Form (10), von deren Koeffizienten das Gleiche gilt, wie von den Koeffizienten h_i, und somit ist ω eine algebraische Zahl.

Zusatz: Sind insbesondere $\alpha, \beta, \cdots, \gamma$ *ganze* algebraische Zahlen, so ist auch ω eine *ganze* algebraische Zahl. Denn in dieser Voraussetzung sind die $A_i, B_i, \cdots, C_i$ rationale ganze Zahlen, womit dann auch die Koeffizienten h_i und endlich auch die Koeffizienten H_i der Gleichung (10), welcher ω genügt, zu *ganzen* Zahlen werden.

Hiernach wird z. B., so oft α eine ganze algebraische Zahl ist, $\sqrt[r]{\alpha^s}$, welche positiven ganzen Zahlen unter r, s auch verstanden werden, als Wurzel der Gleichung

$$x^r - \alpha^s = 0$$

eine ganze algebraische Zahl.

4. Den Sätzen der Nr. 2 zufolge bilden die sämtlichen algebraischen Zahlen eine Gesamtheit von Zahlen von der ausgezeichneten Eigenschaft, daß jede rationale ganzzahlige Funktion von einer oder mehreren Zahlen

der Gesamtheit wieder zu derselben gehört. Eine solche Gesamtheit von Zahlen nennt man nach dem Vorgange von Dedekind *einen Zahlenkörper* oder kurz *einen Körper*.

Alle algebraischen Zahlen bilden also einen Körper.

Solcher Körper gibt es eine unendliche Mannigfaltigkeit. Der einfachste von allen wird nur von einer einzigen Zahl, der Null, gebildet; doch soll in der Folge von diesem nur uneigentlichen Körper vollständig abgesehen oder stets vorausgesetzt werden, daß nicht sämtliche Zahlen des Körpers Null seien. Dann wird der elementarste von allen übrigen der Körper R der rationalen Zahlen sein, deren Gesamtheit offenbar die charakteristische Eigenschaft eines Zahlenkörpers besitzt. Man darf ihn als den elementarsten bezeichnen, da er, wie leicht zu erkennen, in jedem möglichen andern Zahlenkörper enthalten ist, selbst also keinen Zahlenkörper mehr (außer der Null) in sich enthält. In der Tat, jeder mögliche von Null verschiedene Körper enthält mindestens eine von Null verschiedene Zahl α, folglich auch die Zahl $\frac{\alpha}{\alpha} = 1$ und daher auch die Gesamtheit aller rationalen Zahlen.

Allgemein wird ein Körper, dessen sämtliche Zahlen auch in einem andern Körper enthalten sind, ein Teiler des letztern oder auch ein Unterkörper desselben, dieser ein Oberkörper des erstern genannt. Der Körper R der rationalen Zahlen ist also Teiler jedes möglichen Körpers.

Sind andererseits $\mathfrak{K}'$, $\mathfrak{K}''$ irgend zwei gegebene Zahlenkörper, so bildet ersichtlich die Gesamtheit aller Zahlen, welche auf rationale Weise aus Zahlen dieser Körper und ganzen Zahlen gebildet werden können, wieder einen Zahlenkörper $\mathfrak{K}$, in welchem die gegebenen Körper $\mathfrak{K}'$, $\mathfrak{K}''$ als Teiler enthalten sind. Dieser Körper $\mathfrak{K}$ ist zugleich von allen Körpern, die sie beide enthalten, der kleinste, denn zugleich mit ihren Zahlen müßte jeder andere von diesen Zahlenkörpern auch alle aus solchen Zahlen auf rationale Weise gebildeten Zahlen, d. h. die Zahlen des Körpers $\mathfrak{K}$ in sich enthalten. Man nennt daher den Körper $\mathfrak{K}$ das kleinste gemeinsame Vielfache oder auch das Produkt der Körper $\mathfrak{K}'$, $\mathfrak{K}''$ oder sagt: $\mathfrak{K}$ sei aus $\mathfrak{K}'$, $\mathfrak{K}''$

zusammengesetzt, und bezeichnet diesen Umstand durch die Gleichung

$$\mathfrak{K} = \mathfrak{K}' \cdot \mathfrak{K}'' = \mathfrak{K}'' \cdot \mathfrak{K}'.$$

Offenbar besteht für jeden Körper $\mathfrak{K}$ die Beziehung

$$\mathfrak{K}\mathfrak{K}' = \mathfrak{K}'\mathfrak{K} = \mathfrak{K}, \tag{11}$$

so oft $\mathfrak{K}'$ ein Teiler von $\mathfrak{K}$; insbesondere ist also immer

$$\mathfrak{K}R = R\mathfrak{K} = \mathfrak{K}; \tag{12}$$

und auch umgekehrt ist aus der Beziehung (11), wenn sie stattfindet, $\mathfrak{K}'$ als ein Teiler von $\mathfrak{K}$ zu erschließen.

Auch die Gesamtheit aller Zahlen, welche zwei gegebenen Zahlenkörpern $\mathfrak{K}'$, $\mathfrak{K}''$ gemeinsam sind, zu welcher nach dem Gesagten die rationalen Zahlen immer gehören, bildet ersichtlich einen Körper, da, wenn α, β zwei Zahlen bedeuten, die ihr angehören, auch $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$, die sowohl zu $\mathfrak{K}'$ als zu $\mathfrak{K}''$ gehören, in der gedachten Gesamtheit enthalten sein werden. Der so gebildete Körper kann der größte gemeinsame Teiler von $\mathfrak{K}'$, $\mathfrak{K}''$ genannt werden, da offenbar jeder ihnen gemeinsame Körper ein Unterkörper desselben sein muß.

Um andere Körper, als die bisher erkannten, zu bilden, denke man sich eine endliche Anzahl irgend welcher Größen $\mathfrak{R}'$, $\mathfrak{R}''$, $\cdots$ gegeben; diese Größen mögen bestimmte algebraische Zahlen oder auch unbestimmte oder veränderliche Größen $u, v, w, \cdots$ oder auch teilweise das eine, teilweise das andere sein. Dann bildet die Gesamtheit aller Größen, welche aus $\mathfrak{R}'$, $\mathfrak{R}''$, $\cdots$ und ganzen Zahlen oder, was dasselbe sagt, welche aus

$$1, \mathfrak{R}', \mathfrak{R}'', \cdots \tag{13}$$

auf rationale Weise gebildet werden können, ersichtlich einen Körper, welchen wir mit Kronecker[1]) den Rationalitätsbereich

---

1) L. Kronecker, Festschrift zu Herrn E. E. Kummers Doktor-Jubiläum, 10. September 1881, abgedruckt im J. f. Math. 92, p. 1. Der Rationalitätsbereich $\mathfrak{R}$ bildet nicht immer, nämlich nur dann einen Zahlenkörper in dem zuvor definierten Sinne, wenn die Elemente (13)

$$(14)\qquad \mathfrak{R} = (\mathfrak{R}', \mathfrak{R}'', \cdots)$$

nennen wollen. Er wird, wenn die Reihe (13) sich auf ihr Anfangsglied reduziert, zum Körper R aller rationalen Zahlen, kommt, wenn $\mathfrak{R}', \mathfrak{R}'', \cdots$ nur Unbestimmte bezeichnen, mit der Gesamtheit aller rationalen ganzzahligen Funktionen dieser Unbestimmten, z. B. mit der Gesamtheit aller solcher Funktionen einer Veränderlichen z überein, falls die Reihe (13) auf die zwei Glieder $1, z$ sich beschränkt. Werden aus dem Rationalitätsbereiche $\mathfrak{R}$ diejenigen Größen ausgesondert, welche ganze, ganzzahlige Funktionen von $\mathfrak{R}', \mathfrak{R}'', \cdots$ sind, d. h. aus den Größen (13) nur mittels Additionen, Subtraktionen und Multiplikationen gebildet werden können, so wird deren Gesamtheit nach Kronecker der Integritätsbereich von $\mathfrak{R}$ genannt.

Die so gewonnene allgemeine Vorstellung eines bestimmten Rationalitätsbereiches gestattet uns vor allem, die in den vorigen Nummern aufgestellten Sätze sehr erheblich zu verallgemeinern. Man denke sich die Koeffizienten der Gleichung (1) als solche, die dem Rationalitätsbereiche $\mathfrak{R}$ oder seinem Integritätsbereiche angehören, so wollen wir jede Wurzel der Gleichung als eine algebraische bezw. ganze algebraische Funktion von $\mathfrak{R}', \mathfrak{R}'', \cdots$ oder auch als eine in $\mathfrak{R}$ algebraische bezw. ganze algebraische Zahl[1]) bezeichnen. Werden nun die Koeffizienten A_i, B_i in den Gleichungen (4), desgleichen die in Nr. 3 mit $A_i, B_i, \cdots, C_i$ bezeichneten Koeffizienten als zu $\mathfrak{R}$ gehörig vorausgesetzt, so übersieht man, unter dieser Voraussetzung die dort angestellten Betrachtungen wiederholend, sofort, daß auch die Größen $h_k^{(i)}$ sowie endlich die Größen H_i demselben Rationalitätsbereiche $\mathfrak{R}$ angehören müssen; sind insbesondere jene Koeffizienten Glieder des zu $\mathfrak{R}$ gehörigen Integritätsbereiches, so wird von den

---

selbst Zahlen sind, andernfalls, wenn nämlich unter ihnen sich Veränderliche oder Unbestimmte finden, bildet er eine Gesamtheit von Größen allgemeinerer Art, welche die charakteristische Eigenschaft des Zahlenkörpers teilt. Da wir später ausschließlich von dem Falle zu handeln haben, wo $\mathfrak{R}$ nur aus Zahlen besteht, so werden von vornherein die im Körper enthaltenen Größen auch wohl als Zahlen bezeichnet werden.

1) Man beachte die vorige Anmerkung.

Koeffizienten H_i ersichtlich das Gleiche gelten. So erhält man die folgenden allgemeineren Sätze:

Sind α, β zwei identische oder verschiedene in $\mathfrak{R}$ algebraische Zahlen, so sind es auch $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$, letztere Zahl wenigstens dann, wenn β von Null verschieden ist; die Gesamtheit aller in $\mathfrak{R}$ algebraischen Zahlen ist demnach ein Körper. Sind insbesondere α, β zwei in $\mathfrak{R}$ ganze algebraische Zahlen, so gilt von $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ dasselbe.

In entsprechender Weise verallgemeinern sich die Sätze in Nr 3.

5. Wir wenden uns jetzt der Voraussetzung zu, daß der Reihe (13) noch eine in $\mathfrak{R}$ algebraische Zahl α hinzugefügt oder, wie man zu sagen pflegt, adjungiert wird; der aus dieser Annahme entstehende umfassendere Rationalitätsbereich oder Körper, welcher $\mathfrak{R}$ in sich enthält, soll $K(\alpha; \mathfrak{R})$ genannt und zunächst seine allgemeine Gestalt ermittelt werden. Die den Körper $K(\alpha; \mathfrak{R})$ erzeugende Zahl α genügt als eine in $\mathfrak{R}$ algebraische Zahl einer Gleichung mit Koeffizienten, welche in $\mathfrak{R}$ enthalten sind; da es aber möglich ist, daß sie mehr als einer solchen Gleichung Genüge leistet, wählen wir eine derjenigen von ihnen aus, deren Grad möglichst klein ist, und bezeichnen sie mit

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0, \tag{15}$$

sodaß identisch

$$\alpha^n + a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \cdots + a_n = 0 \tag{16}$$

ist. Der Gleichung (15) kommt eine Eigenschaft zu, die wir vor allem hervorheben müssen. Um sie kurz aussprechen zu können, setzen wir einen wichtigen Begriff fest durch folgende Definition[1]): Ist

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

eine ganze Funktion von x, deren Koeffizienten einem gegebenen Rationalitätsbereiche $\mathfrak{R}$ angehören, so soll diese Funktion in $\mathfrak{R}$ *irreduktibel* heißen, wenn sie

1) Vgl. zu den folgenden Betrachtungen Kap. 3 Nr. 1.

nicht in zwei Faktoren geringeren, aber von Null verschiedenen Grades zerlegt werden kann, deren Koeffizienten demselben Rationalitätsbereiche $\mathfrak{R}$ angehörig sind. Zugleich heiße dann die *Gleichung*

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

eine in $\mathfrak{R}$ irreduktible. Ist insbesondere $\mathfrak{R}$ der Bereich R aller rationalen Zahlen, so heißt dann die gedachte Funktion bezw. Gleichung *schlechthin* irreduktibel. Dementsprechend dürfen wir sagen: die Gleichung (15) sei in $\mathfrak{R}$ irreduktibel; denn, zerfiele ihre linke Seite, welche kurz $f(x)$ heiße, in zwei Faktoren geringeren Grades mit gleichfalls in $\mathfrak{R}$ enthaltenen Koeffizienten,

$$f(x) = \varphi(x) \cdot \psi(x),$$

so müßte die Zahl α wenigstens einer der beiden Gleichungen

$$\varphi(x) = 0, \quad \psi(x) = 0$$

Genüge leisten, was der Bedeutung der Funktion $f(x)$ widerspricht.

Nun gelten bezüglich irreduktibler Funktionen und Gleichungen einige allgemeine Sätze, die zunächst hergeleitet werden mögen.

1) Ist $f(x) = 0$ eine in $\mathfrak{R}$ irreduktible Gleichung und $F(x) = 0$ eine andere Gleichung, deren Koeffizienten gleichfalls dem Bereiche $\mathfrak{R}$ angehören, so haben die beiden Gleichungen entweder keine Wurzel gemeinsam, oder alle Wurzeln der ersteren Gleichung genügen auch der zweiten.

Man leite nämlich, indem man zunächst $f(x)$, $F(x)$ als zwei ganz beliebige ganze Funktionen mit Koeffizienten aus dem Bereiche $\mathfrak{R}$ voraussetzt, ganz analog dem Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier ganzen Zahlen durch algebraische Divisionen für die gedachten Funktionen eine Reihe von Gleichungen her von der Form:

$$\begin{aligned} F(x) &= q(x) \cdot f(x) + f_1(x) \\ f(x) &= q_1(x) \cdot f_1(x) + f_2(x) \\ &\cdots\cdots\cdots\cdots, \end{aligned}$$

in welchen die Zeichen $q(x)$, $q_1(x)$, $\cdots$, $f_1(x)$, $f_2(x)$, $\cdots$ lauter

ganze Funktionen mit in $\Re$ enthaltenen Koeffizienten bedeuten, und zwar die letztgenannten Funktionen solche von absteigenden Graden; aus diesem Grunde wird der Algorithmus auf eine letzte Gleichung derselben Gestalt führen, welche

$$f_{i-1}(x) = q_i(x) \cdot f_i(x) + f_{i+1}(x)$$

heiße, während nun bei Fortsetzung der Division sich

$$f_i(x) = q_{i+1}(x) \cdot f_{i+1}(x)$$

und demnach $f_{i+1}(x)$ sich als ein gemeinsamer Teiler aller vorhergehenden Funktionen $f_i(x), f_{i-1}(x), \cdots,$ endlich auch von $f(x)$ ergibt. Aus der Reihe dieser Gleichungen erschließt man ohne Mühe eine Beziehung von der Gestalt:

$$F(x) \cdot P(x) + f(x) \cdot Q(x) = f_{i+1}(x), \tag{17}$$

in welcher $P(x)$, $Q(x)$ ganze Funktionen von x sind, deren Koeffizienten gleich wie diejenigen von $f_{i+1}(x)$ zum Rationalitätsbereiche $\Re$ gehören. — Wird nun die Funktion $f(x)$ als in $\Re$ irreduktibel vorausgesetzt, so kann, weil sie keine Funktion geringeren Grades zum Teiler hat, welche in $\Re$ rationale Koeffizienten besitzt, $f_{i+1}(x)$ nur entweder eine in $\Re$ enthaltene, von Null verschiedene Zahl C, oder bis auf einen solchen Faktor C gleich $f(x)$ sein. Im erstern Falle bestände eine Gleichung

$$F(x) \cdot P(x) + f(x) \cdot Q(x) = C, \tag{18}$$

im andern Falle reduzierte sich die ganze Reihe der Gleichungen auf die erste von ihnen und diese auf die Gestalt

$$F(x) = q(x) \cdot f(x). \tag{18a}$$

In jenem Falle haben also die Gleichungen

$$f(x) = 0, \quad F(x) = 0$$

keine gemeinsame Wurzel, denn für eine solche ergäbe die Gleichung (18) den Widerspruch $0 = C$; in diesem Falle ist $F(x)$ teilbar durch $f(x)$ und demnach jede Wurzel der ersten Gleichung auch eine solche der zweiten.

Da dieser zweite Fall gewiß nicht stattfindet, wenn $F(x)$ geringeren Grades ist als $f(x)$, so folgt der weitere Satz:

2) Eine irreduktible Gleichung hat mit einer Gleichung geringeren Grades, deren Koeffizienten zu dem-

selben Rationalitätsbereiche gehören wie die ihrigen, keine Wurzel gemeinsam.

3) Die Wurzeln jeder irreduktiblen Gleichung sind von einander verschieden. Denn, wäre α eine mehrfache Wurzel einer irreduktibeln Gleichung

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0, \tag{19}$$

so müßte sie bekanntlich auch der abgeleiteten Gleichung

$$n x^{n-1} + (n-1) a_1 x^{n-2} + \cdots + 1 \cdot a_{n-1} = 0 \tag{20}$$

Genüge leisten, deren Koeffizienten demselben Rationalitätsbereiche angehören, wie die der ersteren, deren Grad aber geringer ist, als der ihrige, was nicht sein kann.

4) Hat die in $\mathfrak{R}$ rationale Gleichung $F(x) = 0$ eine Wurzel mit der in demselben Rationalitätsbereiche irreduktiblen Gleichung $f(x) = 0$ gemeinsam, hat sie also alle ihre Wurzeln, zugleich aber keine anderen als sie, so ist $F(x)$ bis auf einen konstanten zu $\mathfrak{R}$ gehörigen Faktor eine Potenz von $f(x)$. Denn in diesem Falle besteht die Gleichung (18^a), in ihr aber hätte der Faktor $q(x)$, wenn er von einer in $\mathfrak{R}$ enthaltenen Konstanten verschieden ist, eine Wurzel mit $f(x)$ gemeinsam, wäre also wieder teilbar durch $f(x)$ usw.

6. Aus diesen Sätzen erschließt man sogleich, daß die von der Zahl α befriedigte in $\mathfrak{R}$ rationale Gleichung (15) niedrigsten Grades völlig eindeutig bestimmt ist. Wäre nämlich $F(x) = 0$ eine andere in $\mathfrak{R}$ rationale Gleichung desselben Grades, der α genügt, so könnte $F(x)$, da $f(x)$ irreduktibel ist, von $f(x)$ nur um einen konstanten Faktor unterschieden und auch dieser nur gleich 1, mithin $F(x) = f(x)$ sein, wenn, wie wir übereinkamen immer zu tun, der Koeffizient des höchsten Gliedes der Gleichungen als Eins gedacht wird. Da mit der Gleichung (15) zugleich auch ihr Grad n völlig eindeutig bestimmt, der Zahl α also charakteristisch ist, soll diese Zahl dann eine in $\mathfrak{R}$ algebraische Zahl n^{ten} Grades genannt werden.

Nun ist jede im Körper $K(\alpha; \mathfrak{R})$ enthaltene Größe, d. i. jeder aus den Elementen

$$\alpha, 1, \mathfrak{R}', \mathfrak{R}'', \cdots$$

rational gebildete Ausdruck entweder eine ganze Funktion von α mit Koeffizienten aus dem Bereiche $\mathfrak{R}$ oder der Quotient zweier solcher Funktionen:

$$\frac{\varphi(\alpha)}{F(\alpha)}, \tag{21}$$

dessen Nenner von Null verschieden; aus diesem Grunde kann $F(x)$ nicht durch $f(x)$ teilbar sein, mithin besteht eine Gleichung von der Form (18), aus welcher für $x = \alpha$ sich

$$\frac{1}{F(\alpha)} = \frac{P(\alpha)}{C},$$

d. h. als eine ganze Funktion von α ergibt, deren Koeffizienten wieder zu $\mathfrak{R}$ gehören; demnach ließe auch der Quotient (21) also allgemein jede in $K(\alpha; \mathfrak{R})$ enthaltene Größe sich als eine ganze Funktion derselben Art darstellen, deren Grad nun, ohne daß die Koeffizienten aufhörten zu $\mathfrak{R}$ zu gehören, mittels der Identität (16) unter den n^{ten} erniedrigt werden kann. Somit ergibt sich, daß jede in $K(\alpha; \mathfrak{R})$ enthaltene Größe ζ sich in die Gestalt

$$\zeta = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1} \tag{22}$$

bringen läßt, in welcher die Koeffizienten r_i dem gegebenen Rationalitätsbereiche $\mathfrak{R}$ angehörig sind. Da aber auch umgekehrt dieser Ausdruck (22), welche zu $\mathfrak{R}$ gehörigen Werte den Koeffizienten r_i auch beigelegt werden, eine Größe des Körpers $K(\alpha; \mathfrak{R})$ sein wird, so *repräsentiert* der mit ζ bezeichnete Ausdruck den gedachten Körper, d. h. er liefert sämtliche Größen desselben und nur solche, wenn darin für die Koeffizienten r_i alle möglichen Zahlen des Rationalitätsbereiches $\mathfrak{R}$ gewählt werden.

Er liefert aber zudem jede Größe des Körpers auch nur einmal. Denn wegen der Irreduktibilität der Gleichung (15) können zwei Ausdrücke von der Gestalt (22) einander nur gleich sein, wenn sie identisch, nämlich die entsprechenden Koeffizienten r_i einander gleich sind.

Somit stellt der Ausdruck (22) die in $K(\alpha; \mathfrak{R})$ gewiß enthaltene Zahl Null nur dann dar, wenn sämtliche Koeffizienten r_i der Null gleich gewählt werden.

7. Dies führt uns natürlicherweise zu einer neuen allgemeinen Begriffsbildung.

Man nennt eine Anzahl gegebener Größen $\omega_1, \omega_2, \cdots, \omega_n$ bezüglich $\mathfrak{R}$ von einander unabhängig, wenn die Beziehung

$$\rho_1\omega_1 + \rho_2\omega_2 + \cdots + \rho_n\omega_n = 0 \tag{23}$$

für kein System von Zahlen ρ_i des Bereiches $\mathfrak{R}$ stattfindet, außer für

$$\rho_1 = \rho_2 = \cdots = \rho_n = 0;$$

andernfalls heißen jene Größen bezüglich $\mathfrak{R}$ von einander abhängig.

Dementsprechend wären die zuvor betrachteten Potenzen

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$$

n bezüglich $\mathfrak{R}$ von einander unabhängige Zahlen.

Bildet man vermittels solcher n unabhängigen Größen $\omega_1, \omega_2, \cdots, \omega_n$ ebensoviel lineare Ausdrücke

$$\left\{\begin{array}{l} \omega_1' = \rho_1'\,\omega_1 + \rho_2'\,\omega_2 + \cdots + \rho_n'\,\omega_n \\ \omega_2' = \rho_1''\,\omega_1 + \rho_2''\,\omega_2 + \cdots + \rho_n''\,\omega_n \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \omega_n' = \rho_1^{(n)}\omega_1 + \rho_2^{(n)}\omega_2 + \cdots + \rho_n^{(n)}\omega_n, \end{array}\right. \tag{24}$$

deren Koeffizienten $\rho_k^{(i)}$ zu $\mathfrak{R}$ gehören, so werden die n Größen $\omega_1', \omega_2', \cdots, \omega_n'$ bezüglich $\mathfrak{R}$ von einander abhängig oder unabhängig sein, jenachdem die Determinante der Gleichungen (24):

$$\mathsf{P} = \begin{vmatrix} \rho_1' & \rho_2' & \cdots & \rho_n' \\ \rho_1'' & \rho_2'' & \cdots & \rho_n'' \\ \cdot & \cdot & \cdot & \cdot \\ \rho_1^{(n)} & \rho_2^{(n)} & \cdots & \rho_n^{(n)} \end{vmatrix} \tag{25}$$

gleich Null oder von Null verschieden ist. Um dies zu beweisen, schicken wir einen Hilfssatz voraus, der uns nebst seinen Verallgemeinerungen in der Folge vielfach von Nutzen sein wird.

Hilfssatz. Ist die aus lauter in $\mathfrak{R}$ rationalen, nämlich zu $\mathfrak{R}$ gehörigen Zahlen c_{ik} gebildete Determinante

$$C = \begin{vmatrix} c_{11} & c_{21} & \cdots & c_{n1} \\ c_{12} & c_{22} & \cdots & c_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ c_{1n} & c_{2n} & \cdots & c_{nn} \end{vmatrix} \tag{26}$$

gleich Null, so lassen sich n Zahlen $x_1, x_2, \cdots, x_n$, die nicht sämtlich gleich Null sind, in $\mathfrak{R}$ so wählen, daß die n Gleichungen

$$c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n = 0 \quad (i = 1, 2, \cdots, n) \tag{27}$$

erfüllt sind. Dies leuchtet von selbst ein, wenn die sämtlichen Elemente c_{ik} der Determinante gleich Null sind. Entgegengesetzten Falls gibt es mindestens eine Unterdeterminante von C, welche nicht gleich Null ist, während alle Unterdeterminanten höheren Grades — nämlich äußersten Falles die Determinante C selbst — gleich Null sind; um die Begriffe zu fixieren, sei etwa

$$C' = \begin{vmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdot & \cdot & \cdot & \cdot \\ c_{1m} & c_{2m} & \cdots & c_{mm} \end{vmatrix}$$

eine solche Unterdeterminante. Entwickelt man dann die Determinante

$$C'' = \begin{vmatrix} c_{11} & c_{21} & \cdots & c_{m1} & u_1 \\ c_{12} & c_{22} & \cdots & c_{m2} & u_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{1,m+1} & c_{2,m+1} & \cdots & c_{m,m+1} & u_{m+1} \end{vmatrix}.$$

nach den Elementen der letzten Vertikalreihe, so daß

$$C'' = u_1 C_1 + u_2 C_2 + \cdots + u_m C_m + u_{m+1} C_{m+1}$$

und hierin $C_{m+1} = \pm C'$ ist, so erkennt man sofort, daß dieser Ausdruck gleich Null wird, sobald man

$$u_1 = c_{i1}, \; u_2 = c_{i2}, \cdots, u_{m+1} = c_{i,m+1} \quad (i = 1, 2, \cdots, n)$$

einsetzt, da so C'' entweder, wenn $i \overline{\gtrless} m$, zwei gleiche Vertikalreihen hätte, oder andernfalls eine der Unterdeterminanten $m + 1^{\text{ten}}$ Grades von C würde, der Annahme gemäß also verschwände. Daher werden offenbar die Gleichungen (27) erfüllt sein, wenn man den Größen x_i die Werte gibt:

$$x_1 = C_1, \; x_2 = C_2, \cdots, x_{m+1} = C_{m+1}, \; x_{m+2} = 0, \cdots, x_n = 0,$$

welche zu $\mathfrak{R}$ gehören, aber nicht sämtlich gleich Null sind, da $C_{m+1} = \pm C'$ von Null verschieden vorausgesetzt ist.

Sind insbesondere die Elemente c_{ik} der Determinante C Größen des zu $\mathfrak{R}$ gehörigen Integritätsbereiches, so zeigt diese Bestimmung der Größen x_i, daß auch sie dem Integritätsbereiche entnommen werden können. So werden sie als rationale ganze Zahlen bestimmbar sein, wenn die c_{ik} sämtlich rationale ganze Zahlen sind.

Man übersieht ferner sofort, daß in diesem Falle die angestellte Betrachtung und somit der Satz auch gültig bleibt, wenn überall statt der Gleichheit die Kongruenz nach einem beliebigen ganzzahligen Modulus gesetzt wird.

Wären andererseits die Elemente c_{ik} der Determinante C, statt ganze Zahlen zu sein, ganze ganzzahlige Funktionen von beliebig viel Unbestimmten $u, v, \cdots$, so würde auch die Determinante C eine solche Funktion, das von uns angestellte Räsonnement sich aber auch auf diese Voraussetzung sofort übertragen lassen; man gewinnt also noch eine weitere Verallgemeinerung des Hilfssatzes, die wir folgendermaßen aussprechen können:

Ist die aus lauter ganzen ganzzahligen Funktionen der Unbestimmten $u, v, \cdots$ gebildete Determinante C, nämlich jeder Koeffizient der ihr gleichen Funktion von $u, v, \cdots$ gleich bezw. nach einem beliebig gegebenen ganzzahligen Modulus kongruent Null, so lassen sich n ganze ganzzahlige Funktionen $x_1, x_2, \cdots, x_n$ der Unbestimmten $u, v, \cdots$, die nicht sämtlich gleich bezw. kongruent Null sind, so bestimmen, daß die n Ausdrücke

$$c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n \tag{28}$$
$$(i = 1, 2, \cdots, n)$$

gleich bezw. kongruent Null werden.

Auf Grund dieses Hilfssatzes erkennt man nun sogleich, daß, wenn die Determinante P gleich Null ist, sich n zu $\mathfrak{R}$ gehörige Zahlen $\varrho_1, \varrho_2, \cdots, \varrho_n$ angeben lassen, die nicht sämtlich verschwinden, derart, daß die n Gleichungen:

$$\varrho_1\varrho_i' + \varrho_2\varrho_i'' + \cdots + \varrho_n\varrho_i^{(n)} = 0 \tag{29}$$
$$(i = 1, 2, \cdots, n)$$

erfüllt sind, infolge deren dann aus (24) sich auch die Gleichung

$$\varrho_1\omega_1' + \varrho_2\omega_2' + \cdots + \varrho_n\omega_n' = 0 \tag{30}$$

ergibt; mithin sind dann die n Größen $\omega_1', \omega_2', \cdots, \omega_n'$ bezüglich $\mathfrak{R}$ voneinander abhängig. Ist dagegen P eine von Null verschiedene, offenbar zu $\mathfrak{R}$ gehörige Größe, so kann eine Gleichung (30) für zu $\mathfrak{R}$ gehörige ϱ_i nur bestehen, wenn diese Größen sämtlich Null sind, denn aus ihr ergeben sich, wenn die Ausdrücke (24) eingesetzt werden, mit Rücksicht auf die bezüglich $\mathfrak{R}$ vorausgesetzte Unabhängigkeit der Größen $\omega_1, \omega_2, \cdots, \omega_n$ die n Gleichungen (29) und, da deren Determinante nicht Null, die Werte $\varrho_1 = \varrho_2 = \cdots = \varrho_n = 0$; in diesem Falle sind also $\omega_1', \omega_2', \cdots, \omega_n'$ bezüglich $\mathfrak{R}$ voneinander unabhängige Größen. Der behauptete Satz ist also bewiesen.

8. Ist nun ein Zahlenkörper $\mathfrak{K}$ so beschaffen, daß er n bezüglich eines gegebenen Rationalitätsbereiches $\mathfrak{R}$ unabhängige Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ enthält, daß aber je $n+1$ seiner Zahlen bezüglich $\mathfrak{R}$ voneinander abhängig sind, so nennen wir ihn einen bezüglich $\mathfrak{R}$ endlichen Körper n^{ten} Grades (Dedekind).

Da dieser Definition zufolge zwischen jeder Zahl ζ des Körpers und den n Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ desselben eine Beziehung besteht von der Gestalt

$$\varrho\zeta + \varrho_1\omega_1 + \varrho_2\omega_2 + \cdots + \varrho_n\omega_n = 0,$$

in welcher die Koeffizienten zu $\mathfrak{R}$ gehörige Größen sind, unter denen insbesondere ϱ wegen der vorausgesetzten Unabhängigkeit der Zahlen ω_i nicht Null sein kann, so ergibt sich die Folgerung:

Jede Zahl ζ des Körpers $\mathfrak{K}$ läßt sich darstellen in der Form:

$$\zeta = r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n, \tag{31}$$

wo die Koeffizienten r_i in $\mathfrak{R}$ enthalten sind.

Mit bezug hierauf sollen die Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ *eine Basis* des Körpers $\mathfrak{K}$ heißen. Zwecks einer solchen allgemeinen Darstellung seiner Zahlen ζ dürfen sie durch je n andere bezüglich $\mathfrak{R}$ unabhängige Zahlen des Körpers ersetzt werden. Je n solcher Zahlen $\omega_1', \omega_2', \cdots, \omega_n'$ sind durch Gleichungen von der Gestalt der Gleichungen (24) bestimmt, deren Determinante P von Null verschieden ist; und umgekehrt werden n durch solche Gleichungen bestimmte Zahlen, falls

sie dem Körper angehören, n bezüglich $\mathfrak{R}$ unabhängige Zahlen desselben sein. Man erhält demnach sämtliche Basen des Körpers aus einer solchen Basis $\omega_1, \omega_2, \cdots, \omega_n$, wenn man diejenigen Systeme (24) von n Zahlen $\omega_1', \omega_2', \cdots, \omega_n'$ desselben bildet, für welche die Determinante P von Null verschieden ist.

Für unsere späteren Untersuchungen dürfen wir uns auf den Fall beschränken, in welchem der Rationalitätsbereich $\mathfrak{R}$ selbst im Körper $\mathfrak{K}$ enthalten ist. Machen wir also von nun an diese Voraussetzung, so wird nicht nur jede Zahl ζ des Körpers von der Form (31), sondern auch umgekehrt jede durch diese Form gelieferte Zahl ζ eine Zahl des Körpers sein. In dieser Voraussetzung *repräsentiert* daher die Formel (31) den gesamten Körper $\mathfrak{K}$ in eindeutiger Weise.

Da mit ζ zugleich auch die Produkte $\zeta\omega_1, \zeta\omega_2, \cdots, \zeta\omega_n$ zu $\mathfrak{K}$ gehören, lassen sich analog mit (31) n Gleichungen aufstellen von folgender Gestalt:

$$\zeta\omega_i = r_{i1}\omega_1 + r_{i2}\omega_2 + \cdots + r_{in}\omega_n, \quad (i = 1, 2, \cdots, n) \tag{32}$$

wo die sämtlichen Koeffizienten r_{ik} in $\mathfrak{R}$ enthalten sind. Gibt man ihnen die Form

$$\tag{32a} \begin{cases} 0 = (r_{11} - \zeta)\,\omega_1 + r_{12}\omega_2 + \cdots + r_{1n}\omega_n \\ 0 = r_{21}\omega_1 + (r_{22} - \zeta)\,\omega_2 + \cdots + r_{2n}\omega_n \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ 0 = r_{n1}\omega_1 + r_{n2}\omega_2 + \cdots + (r_{nn} - \zeta)\,\omega_n \end{cases}$$

und bedenkt, daß nicht sämtliche Basiszahlen gleich Null sein können, da nach der stets von uns gemachten Voraussetzung der Körper $\mathfrak{K}$ auch Zahlen enthält, die von Null verschieden sind, so folgt aus dem vorigen Systeme von Gleichungen diese andere:

$$(-1)^n \cdot \varphi(\zeta) = \begin{vmatrix} r_{11} - \zeta, & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} - \zeta & \cdots & r_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ r_{n1} & r_{n2} & \cdots & r_{nn} - \zeta \end{vmatrix} = 0, \tag{33}$$

welche, entwickelt, folgendermaßen geschrieben werden kann:

$$\varphi(\zeta) = \zeta^n + R_1\zeta^{n-1} + R_2\zeta^{n-2} + \cdots + R_n = 0; \tag{34}$$

die Koeffizienten R_i gehören ersichtlich wieder zum Rationalitätsbereiche $\mathfrak{R}$. Dieses Resultat spricht sich in dem Satze aus: Jede Zahl ζ des endlichen Körpers $\mathfrak{K}$ ist eine in $\mathfrak{R}$ algebraische Zahl.

Es ist aber wesentlich, zu bemerken, daß die Gleichung, als deren Wurzel sie hier bestimmt worden ist, von der willkürlichen Wahl der Basis, die der Betrachtung zu Grunde lag, nicht abhängt. Seien nämlich die durch die Gleichungen (24) definierten Zahlen $\omega_1', \omega_2', \cdots, \omega_n'$ eine andere Basis des Körpers $\mathfrak{K}$ und

$$\zeta\omega_i' = r_{i1}'\omega_1' + r_{i2}'\omega_2' + \cdots + r_{in}'\omega_n' \qquad (i = 1, 2, \cdots, n) \tag{35}$$

die n den Gleichungen (32) entsprechenden Gleichungen, so ergeben sich statt der Formeln (33) und (34) die folgenden:

$$\begin{vmatrix} r_{11}'-\zeta, & r_{12}' \cdots & r_{1n}' \\ r_{21}' & r_{22}'-\zeta \cdots & r_{2n}' \\ \cdot & \cdot \quad \cdot \quad \cdot & \cdot \\ r_{n1}' & r_{n2}' \cdots & r_{nn}'-\zeta \end{vmatrix} = 0 \tag{36}$$

und

$$\varphi'(\zeta) = \zeta^n + R_1'\zeta^{n-1} + R_2'\zeta^{n-2} + \cdots + R_n' = 0. \tag{37}$$

Wenn man nun sowohl die Gleichung (33) wie (36) mit der von Null verschiedenen Determinante P multipliziert, indem man das erste Mal Kolonnen mit Reihen, das andere Mal Reihen mit Kolonnen verbindet, so wird das allgemeine Glied der entstehenden Determinante das erste Mal

$$C_{ik} = \sum_h r_{hk}\varrho_h^{(i)} - \zeta \cdot \varrho_k^{(i)},$$

das andere Mal

$$C_{ik}' = \sum_h r_{ih}'\varrho_k^{(h)} - \zeta \cdot \varrho_k^{(i)},$$

diese beiden Ausdrücke aber sind gleich. In der Tat, werden die Werte (24) in die Gleichungen (35) eingesetzt, so ergibt sich

$$\zeta \cdot \sum_k \varrho_k^{(i)}\omega_k = \sum_k \left(\omega_k \cdot \sum_h r_{ih}'\varrho_k^{(h)}\right), \qquad (i = 1, 2, \cdots, n)$$

unmittelbar aus den Gleichungen (32) aber folgt

$$\zeta \cdot \sum_k \varrho_k^{(i)}\omega_k = \sum_k \left(\omega_k \cdot \sum_h r_{hk}\varrho_h^{(i)}\right), \qquad (i = 1, 2, \cdots, n)$$

und da diese n Gleichungen mit den vorigen übereinstimmen müssen, die behauptete Gleichheit. Hieraus aber ergibt sich die Identität der beiden Ausdrücke $\varphi(\zeta)$, $\varphi'(\zeta)$.

Demnach ist die Gleichung (34), welche deshalb die für ζ charakteristische Gleichung n^{ten} Grades heißen soll, zugleich mit ihren Koeffizienten nur durch die Zahl ζ selbst bestimmt und daher dürfen diese Koeffizienten als Funktionen von ζ angesehen werden. Wir haben von ihnen besonders den ersten und den letzten ins Auge zu fassen und führen daher für sie besondere Zeichen und Benennungen ein. Wir nennen

$$(38)\qquad (-1)^n \cdot R_n = \begin{vmatrix} r_{11} r_{12} \cdots r_{1n} \\ r_{21} r_{22} \cdots r_{2n} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{n1} r_{n2} \cdots r_{nn} \end{vmatrix}$$

die Norm von ζ, in Zeichen $N(\zeta)$, und

$$(39)\qquad R_1 = r_{11} + r_{22} + \cdots + r_{nn}$$

die Spur von ζ, in Zeichen $S(\zeta)$: die erstere ist nichts anderes als das Produkt, die andere die Summe aller Wurzeln der Gleichung $\varphi(\zeta) = 0$. Sie gehören beide immer dem Rationalitätsbereiche $\mathfrak{R}$, ja sogar, so oft die Größen r_{ik} zu dessen Integritätsbereiche zählen, dem letzteren an. Einige fundamentale Eigenschaften dieser Funktionen sollen sogleich hier zusammengestellt werden.

Aus der Betrachtung der Gleichungen (32) folgt unmittelbar, daß sämtliche r_{ik} gleich Null sind, wenn $\zeta = 0$, desgleichen bis auf die Koeffizienten r_{ii}, welche Eins werden, wenn $\zeta = 1$ ist. Somit findet sich

$$(40)\qquad S(0) = 0, \quad S(1) = n.$$

Bezeichnet ϱ irgend eine Größe des Bereichs $\mathfrak{R}$, so lassen die Gleichungen (32) wieder sogleich erkennen, daß

$$(41)\qquad S(\varrho\zeta) = \varrho \cdot S(\zeta)$$

ist; desgleichen findet sich für zwei beliebige Zahlen ζ', ζ'' des Körpers

$$(42)\qquad S(\zeta' + \zeta'') = S(\zeta') + S(\zeta'').$$

Ebenso unmittelbar ergeben sich die Formeln

$$(43) \qquad N(0) = 0, \quad N(1) = 1,$$

zugleich aber zeigen die Gleichungen (32), daß die Zahl $\zeta = 0$ die einzige ist, deren Norm verschwindet; denn, wird die Determinante (38) der Gleichungen als Null vorausgesetzt, so lassen sich dem Hilfssatze der Nr. 7 zufolge n zu $\mathfrak{R}$ gehörige nicht sämtlich verschwindende Größen $x_1, x_2, \cdots, x_n$ so wählen, daß

$$\zeta(x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n) = 0$$

wird, was $\zeta = 0$ erfordert, da die Größen ω_i in $\mathfrak{R}$ unabhängig voneinander sind.

Ist ζ eine zu $\mathfrak{R}$ gehörige Zahl des Körpers $\mathfrak{K}$, so lehren die Gleichungen (32) wegen dieser Unabhängigkeit der ω_i die neue Beziehung

$$(44) \qquad N(\zeta) = \zeta^n.$$

Ist ferner ζ' eine zweite Zahl des Körpers $\mathfrak{K}$, für welche die mit (32) analogen Gleichungen die folgenden seien:

$$\zeta'\omega_i = r'_{i1}\omega_1 + r'_{i2}\omega_2 + \cdots + r'_{in}\omega_n, \quad (i = 1, 2, \cdots, n)$$

so findet sich

$$\zeta\zeta' \cdot \omega_i = R_{i1}\omega_1 + R_{i2}\omega_2 + \cdots + R_{in}\omega_n, \quad (i = 1, 2, \cdots, n)$$

wenn gesetzt wird

$$R_{ik} = r'_{i1}r_{1k} + r'_{i2}r_{2k} + \cdots + r'_{in}r_{nk};$$

infolge dieser Beziehung ergibt sich die Determinantenrelation

$$|R_{ik}| = |r_{ik}| \cdot |r'_{ik}|, \qquad (i, k = 1, 2, \cdots, n)$$

d. h.

$$(45) \qquad N(\zeta\zeta') = N(\zeta) \cdot N(\zeta').$$

Da mit ζ zugleich auch $\frac{1}{\zeta}$ eine Zahl des Körpers ist (vorausgesetzt, daß ζ nicht Null), findet man hieraus insbesondere für $\zeta' = \frac{1}{\zeta}$ mit Rücksicht auf (43) die Beziehung

$$N(\zeta) \cdot N\left(\frac{1}{\zeta}\right) = 1$$

und ferner

$$N\left(\frac{\zeta'}{\zeta}\right) = \frac{N(\zeta')}{N(\zeta)}.$$

Endlich bemerken wir, daß die Gleichungen (32) folgendermaßen geschrieben werden können:

$$(\zeta - \varrho) \cdot \omega_i = r_{i1}\omega_1 + \cdots + (r_{ii} - \varrho)\omega_i + \cdots + r_{in}\omega_n, \quad (i = 1, 2, \cdots, n)$$

wobei unter ϱ irgend eine zu $\mathfrak{R}$ gehörige Größe gedacht werden soll. Nach der Definition der Norm und der Bedeutung der Funktion $\varphi(\zeta)$ ergibt sich hieraus sogleich nachstehende Formel:

$$N(\zeta - \varrho) = (-1)^n \cdot \varphi(\varrho). \tag{46}$$

Nunmehr seien $\zeta_1, \zeta_2, \cdots, \zeta_n$ irgend welche n Zahlen des Körpers $\mathfrak{K}$, so daß n Gleichungen statthaben von der Form:

$$\zeta_i = r_1^{(i)} \cdot \omega_1 + r_2^{(i)} \cdot \omega_2 + \cdots + r_n^{(i)} \cdot \omega_n, \quad (i = 1, 2, \cdots, n) \tag{47}$$

deren Koeffizienten zu $\mathfrak{R}$ gehören; jenachdem deren Determinante

$$| r_k^{(i)} | \qquad (i, k = 1, 2, \cdots, n)$$

von Null verschieden ist oder nicht, sind die n Zahlen bezüglich $\mathfrak{R}$ unabhängig oder voneinander abhängig und dürfen sie daher entsprechend als eine Basis des Körpers gewählt werden oder nicht. Nun folgt aus den Gleichungen (47)

$$\zeta_i \zeta_k = \sum_{h, h'} r_h^{(i)} r_{h'}^{(k)} \cdot \omega_h \omega_{h'}$$

also mit Beachtung der Formeln (41) und (42) auch

$$S(\zeta_i \zeta_k) = \sum_{h, h'} r_h^{(i)} r_{h'}^{(k)} \cdot S(\omega_h \omega_{h'}). \tag{48}$$

Wenn man daher die Determinante

$$\begin{vmatrix} S(\zeta_1\zeta_1), & S(\zeta_1\zeta_2) \cdots S(\zeta_1\zeta_n) \\ S(\zeta_2\zeta_1), & S(\zeta_2\zeta_2) \cdots S(\zeta_2\zeta_n) \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ S(\zeta_n\zeta_1), & S(\zeta_n\zeta_2) \cdots S(\zeta_n\zeta_n) \end{vmatrix} \tag{49}$$

zur Abkürzung mit dem Zeichen

$$\Delta(\zeta_1, \zeta_2, \cdots, \zeta_n) \tag{50}$$

bezeichnet, so liefert die Formel (48) auf Grund des Multiplikationssatzes für Determinanten die äußerst wichtige Beziehung:

$$\Delta(\zeta_1, \zeta_2, \cdots, \zeta_n) = | r_k^{(i)} |^2 \cdot \Delta(\omega_1, \omega_2, \cdots, \omega_n). \tag{51}$$

Die hier definierte Größe (50) wird die Diskriminante der n Zahlen $\zeta_1, \zeta_2, \cdots, \zeta_n$ des Körpers genannt; man erhält demnach den Satz:

Hängen n Zahlen $\zeta_1, \zeta_2, \cdots, \zeta_n$ des Körpers mit seinen Basiszahlen $\omega_1, \omega_2, \cdots, \omega_n$ durch die Gleichungen (47) zusammen, so ist die Diskriminante der Zahlen gleich dem Produkte aus der Diskriminante der Basis und dem Quadrate der Determinante jener Gleichungen.

Die Diskriminante jeder Basis ist von Null verschieden. Denn, wäre $\Delta(\omega_1, \omega_2, \cdots, \omega_n)$ gleich Null, so ließen sich, da die sämtlichen Spuren $S(\omega_k \omega_{k'})$ zu $\mathfrak{R}$ gehören, nach dem Hilfssatze der Nr. 7 n nicht sämtlich verschwindende Größen $x_1, x_2, \cdots, x_n$ in $\mathfrak{R}$ so wählen, daß die n Gleichungen

$$x_1 \cdot S(\omega_i \omega_1) + x_2 \,.\, S(\omega_i \omega_2) + \cdots + x_n \cdot S(\omega_i \omega_n) = 0$$
$$(i = 1, 2, \cdots, n)$$

oder wegen (41) und (42) die Gleichungen

$$(52) \qquad S\Big(\omega_i(x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n)\Big) = 0$$
$$(i = 1, 2, \cdots, n)$$

erfüllt wären. Setzt man aber

$$\xi = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

eine von Null verschiedene Zahl, welche dem Körper $\mathfrak{K}$ angehört, da auch $\mathfrak{R}$ in ihm enthalten sein soll, und ist

$$\zeta = r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$$

eine beliebige Zahl des Körpers $\mathfrak{K}$, so ergibt sich

$$\xi\zeta = r_1 \cdot \omega_1\xi + r_2 \cdot \omega_2\xi + \cdots + r_n \cdot \omega_n\xi,$$

also müßte mit Rücksicht auf (52) und wegen (41) und (42) die Gleichung

$$S(\xi\zeta) = 0$$

für jede in $\mathfrak{K}$ enthaltene Zahl ζ stattfinden, während sie doch sicher nicht besteht, wenn unter ζ die in $\mathfrak{K}$ enthaltene Zahl $\frac{1}{\xi}$ verstanden wird.

Der in (51) ausgesprochene Satz gestattet, das zuletzt bewiesene Resultat umzukehren und zu sagen: Ist die Diskriminante von n Zahlen $\zeta_1, \zeta_2, \cdots, \zeta_n$ des Körpers von Null verschieden, so bilden sie eine Basis desselben.

Denn alsdann kann wegen (51) die Determinante $|r_k^{(i)}|$ nicht verschwinden, folglich sind die durch die Gleichungen (47) mit der Basis $\omega_1, \omega_2, \cdots, \omega_n$ verbundenen Zahlen $\zeta_1, \zeta_2, \cdots, \zeta_n$ in $\mathfrak{R}$ unabhängige Zahlen des Körpers, mithin auch eine Basis desselben.

Das Nichtverschwinden der Diskriminante von n Zahlen des Körpers ist also die sowohl notwendige als hinreichende Bedingung dafür, daß sie eine Basis des Körpers ausmachen.

9. Von hier an beschränken wir den Rationalitätsbereich $\mathfrak{R}$, wenn nicht ausdrücklich anderes festgesetzt wird, auf den Bereich R der rationalen Zahlen oder auf denjenigen rationaler ganzzahliger Funktionen einer endlichen Anzahl von Unbestimmten $u, v, w, \cdots$. Unter dieser Voraussetzung denken wir uns den in $\mathfrak{R}$ endlichen Körper $\mathfrak{K}$ n^{ten} Grades in der Weise verwandelt, daß an Stelle jeder einzelnen Zahl[1]) α desselben eine bestimmte andere Zahl gedacht werde, welche wir durch den gleichen akzentuierten Buchstaben α' bezeichnen und nicht für alle α gleich Null annehmen wollen. Es soll dabei ausdrücklich festgesetzt werden, daß, wenn der (in $\mathfrak{K}$ enthaltene) Bereich $\mathfrak{R}$ Unbestimmte enthält, jede solche Unbestimmte bei der Verwandlung des Körpers wieder durch eine Unbestimmte ersetzt oder, was auf dasselbe hinauskommt, unveränderlich sein soll. Auch sollen für je zwei Zahlen α, β des Körpers und die ihn ersetzenden Zahlen α', β' die Beziehungen

$$(53) \qquad (\alpha+\beta)' = \alpha' + \beta', \quad (\alpha\beta)' = \alpha' \cdot \beta'$$

vorausgesetzt, d. h. die Summe zweier Zahlen stets in die Summe, ihr Produkt stets in das Produkt der sie ersetzenden Zahlen verwandelt werden. Jede Verwandlung des Körpers $\mathfrak{K}$ nach diesen Regeln soll eine Substitution heißen.

Man erschließt aus den gemachten Festsetzungen zunächst, daß auch

$$(54) \qquad (\alpha-\beta)' = \alpha' - \beta', \quad \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

ist, letzteres wenigstens, so oft β eine von Null verschiedene

1) Wegen des Ausdrucks „Zahl“ s. die Anmerkung auf S. 9.

Zahl des Körpers ist; setzt man nämlich in der ersten der Formeln (53) statt α die ebenfalls in $\mathfrak{K}$ enthaltene Zahl $\alpha - \beta$, so findet sich

$$\alpha' = (\alpha - \beta)' + \beta',$$

d. i. die erste der Formeln (54); setzt man, falls β von Null verschieden, in der zweiten der Formeln (53) statt α die ebenfalls in $\mathfrak{K}$ enthaltene Zahl $\frac{\alpha}{\beta}$, so kommt

$$\alpha' = \left(\frac{\alpha}{\beta}\right)' \cdot \beta'.$$

Nun sind immer zwei entsprechende Zahlen entweder zugleich Null oder zugleich von Null verschieden; denn für $\beta = 0$ gibt die erste der Formeln (53) auch $\beta' = 0$; wäre aber β' für ein von Null verschiedenes β gleich Null, so wäre der letzterhaltenen Gleichung zufolge jede Zahl α' gleich Null gegen unsere Voraussetzung. Somit sind die Formeln (54) bewiesen und aus dem Stattfinden der Gleichungen (53) und (54) erkennt man sofort einerseits, daß die Gesamtheit $\mathfrak{K}'$ der Zahlen α' wieder ein Körper ist, den wir mit dem Körper $\mathfrak{K}$ konjugiert nennen wollen; andererseits, daß jeder aus Zahlen des Körpers $\mathfrak{K}$ rational mit ganzzahligen Koeffizienten gebildete Ausdruck, weil er aus einer endlichen Folge von Additionen, Subtraktionen, Multiplikationen und Divisionen erhalten werden kann, bei der Substitution in den gleichen rationalen aus den entsprechenden Zahlen des konjugierten Körpers $\mathfrak{K}'$ gebildeten Ausdruck übergehen muß.

Da ferner, wenn β mit α identifiziert wird, auch $\beta' = \alpha'$ sein muß, liefert die zweite der Formeln (54) das Resultat $1' = 1$, d. h. die Eins und folglich auch alle rationalen Zahlen bleiben bei jeder Substitution ungeändert. Nach unserer, die etwaigen Unbestimmten betreffenden Festsetzung gilt hiernach dasselbe auch von jeder rationalen ganzzahligen Funktion der im Bereiche $\mathfrak{R}$ vorhandenen Unbestimmten, oder allgemein: **Jede Größe des Rationalitätsbereiches $\mathfrak{R}$ bleibt bei der Substitution des Körpers $\mathfrak{K}'$ an Stelle von $\mathfrak{K}$ ungeändert.**

Endlich entspricht nun auch umgekehrt jeder Zahl des Körpers $\mathfrak{K}'$ eine eindeutig bestimmte Zahl des Körpers $\mathfrak{K}$; denn

entsprächen der Zahl α', die jedenfalls der Ersatz für eine Zahl von $\mathfrak{K}$ sein muß, zwei verschiedene Zahlen α, β desselben, so wäre auch $\beta' = \alpha'$, was doch der ersten der Formeln (54) gemäß nur für $\alpha = \beta$ der Fall sein kann. Diese umgekehrte Beziehung zwischen den Körpern $\mathfrak{K}'$ und $\mathfrak{K}$ ist aber auch eine Substitution; denn offenbar folgen aus den Formeln (53), (54) als die den Zahlen

$$\alpha' + \beta', \quad \alpha' - \beta', \quad \alpha'\beta', \quad \frac{\alpha'}{\beta'}$$

des Körpers $\mathfrak{K}'$ entsprechenden Zahlen resp. die Summe, die Differenz, das Produkt und der Quotient der den Zahlen α', β' entsprechenden Zahlen α, β, nämlich die Zahlen

$$\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad \frac{\alpha}{\beta}\cdot$$

Wir bezeichnen die neue Substitution als die inverse oder reziproke der ersteren. Die beiden Körper $\mathfrak{K}$ und $\mathfrak{K}'$ sind mithin jeder dem andern konjugiert. Die einander entsprechenden Zahlen α, α' beider Körper heißen gleichfalls einander konjugiert.

Machen wir von diesen allgemeinen Betrachtungen eine Anwendung auf den Körper $K(\alpha; \mathfrak{R})$, den wir in Nr. 6 durch die Formel

$$(55) \qquad \zeta = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1}$$

repräsentiert fanden, indem wir unter α eine Wurzel der in $\mathfrak{R}$ irreduktiblen Gleichung n^{ten} Grades

$$(56) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

verstanden, so daß identisch

$$(57) \qquad \alpha^n + a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \cdots + a_n = 0$$

ist. Dieser Körper ist ein in $\mathfrak{R}$ endlicher Körper n^{ten} Grades, denn er enthält nach Anfang von Nr. 7 die n in $\mathfrak{R}$ unabhängigen Größen $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$, aber zwischen je $n+1$ Größen von der Form

$$\zeta_i = r_0^{(i)} + r_1^{(i)}\alpha + r_2^{(i)}\alpha^2 + \cdots + r_{n-1}^{(i)}\alpha^{n-1}$$
$$(i = 1, 2, \cdots, n+1)$$

erhält man durch Elimination von $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ eine Gleichung von der Form

$$\varrho_1\zeta_1 + \varrho_2\zeta_2 + \cdots + \varrho_{n+1}\zeta_{n+1} = 0,$$

deren in $\mathfrak{R}$ rationale Koeffizienten nicht alle verschwinden. Wenn nun S irgend eine Substitution des gedachten Körpers ist, bei welcher α' die α ersetzende Zahl heiße, so geht der Ausdruck zur Linken von (57), da die zu $\mathfrak{R}$ gehörigen Koeffizienten ungeändert bleiben, in den nachstehenden über:

$$\alpha'^n + a_1\alpha'^{n-1} + a_2\alpha'^{n-2} + \cdots + a_n,$$

der aber, weil jener gleich Null und die der Null korrespondierende Zahl, wie bemerkt, stets Null ist, ebenfalls verschwinden muß. Mithin ist die der Zahl α entsprechende Zahl α' bei jeder Substitution eine Wurzel der Gleichung (56); ist sie aber bestimmt, so erhalten wir zugleich alle Zahlen des der Substitution entstammenden konjugierten Körpers $\mathfrak{K}'$ mittels der Formel

$$(58) \qquad \zeta' = r_0 + r_1\alpha' + r_2\alpha'^2 + \cdots + r_{n-1}\alpha'^{n-1},$$

welche dann notwendig durch die Substitution aus (55) hervorgeht. Hiernach gibt es nicht mehr verschiedene Substitutionen für den Körper $K(\alpha; \mathfrak{R})$, als die Anzahl verschiedener Wurzeln der Gleichung (56) beträgt, d. h. da diese irreduktibel ist, die Anzahl n. Jeder dieser n Wurzeln entspricht aber in der Tat eine Substitution. Denn, ersetzt man die Zahl α durch irgend eine der gedachten n Wurzeln α', gleichviel ob sie mit α identisch oder nicht, und läßt allgemeiner jeder Zahl ζ des Körpers $\mathfrak{K}$ die Zahl

$$(59) \qquad \zeta' = r_0 + r_1\alpha' + r_2\alpha'^2 + \cdots + r_{n-1}\alpha'^{n-1}$$

entsprechen, so sind erstens nicht sämtliche ζ' gleich Null, da der Zahl $\zeta = r_0$ für $r_0 \gtrless 0$ die Zahl $\zeta' = r_0$ entspräche; zweitens bleiben hiernach auch die Größen des Rationalitätsbereiches $\mathfrak{R}$ (insbesondere also die darin etwa vorhandenen Unbestimmten) ungeändert; drittens bestehen die Formeln (53), da die der Summe zweier Ausdrücke (55) entsprechende Zahl ersichtlich die Summe der beiden ihnen korrespondierenden Ausdrücke (59) sein wird, das Produkt zweier Ausdrücke (55) aber mittels der Identität (57) wieder auf dieselbe allgemeine Form gebracht werden kann, welcher offenbar derjenige Ausdruck korrespondieren muß, auf welchen das Produkt der jenen entsprechenden beiden Ausdrücke (59) mittels der zu (57) korrespondierenden Identität

$$\alpha'^n + a_1\alpha'^{n-1} + a_2\alpha'^{n-2} + \cdots + a_n = 0$$

zurückführbar ist. Somit ist die gedachte Verwandlung des Körpers $\mathfrak{K}$ eine Substitution, bei welcher natürlich, falls $\alpha' = \alpha$ gedacht wird, jede seiner Zahlen ungeändert bleibt; sie wird infolgedessen alsdann die identische Substitution genannt.

Der Körper $K(\alpha; \mathfrak{R})$ n^{ten} Grades läßt also genau n Substitutionen zu, die man erhält, indem man einfach in der Formel (55) des Körpers die Wurzel α durch die sämtlichen Wurzeln $\alpha, \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n-1)}$ der Gleichung (56) ersetzt. So entstehen n zueinander konjugierte Körper

$$\mathfrak{K}, \mathfrak{K}^{(1)}, \mathfrak{K}^{(2)}, \cdots, \mathfrak{K}^{(n-1)},$$

die freilich sämtlich oder doch teilweise miteinander identisch, nämlich ein und dieselbe Gesamtheit der gleichen, wenn auch anders geordneten Zahlen sein können. Der Körper $\mathfrak{K}$ wird ein Galoisscher Körper genannt, wenn er mit allen seinen Konjugierten identisch ist.

10. Seien jetzt α, A zwei in $\mathfrak{R}$ algebraische Zahlen, die erste vom Grade n und durch die in $\mathfrak{R}$ irreduktible Gleichung

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0 \tag{60}$$

bestimmt, die andere vom Grade N und Wurzel der in $\mathfrak{R}$ irreduktibeln Gleichung

$$x^N + A_1x^{N-1} + A_2x^{N-2} + \cdots + A_N = 0. \tag{61}$$

Die Wurzeln der Gleichung (60) mögen jetzt

$$\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$$

heißen. Dem im Vorigen Entwickelten zufolge entsprechen den beiden Zahlen α, A zwei in $\mathfrak{R}$ endliche Körper

$$\mathfrak{k} = K(\alpha; \mathfrak{R}), \quad \mathfrak{K} = K(\mathsf{A}; \mathfrak{R})$$

von den Graden n, N resp., in denen der Rationalitätsbereich $\mathfrak{R}$ enthalten ist. Wir wollen denjenigen Körper $K = \mathfrak{k} \cdot \mathfrak{K}$ bestimmen, der aus ihnen zusammengesetzt ist; er entsteht offenbar, wenn man dem Rationalitätsbereiche $\mathfrak{k}$ noch die in $\mathfrak{R}$ also auch in $\mathfrak{k}$ algebraische Zahl A adjungiert. Diese Zahl genügt mindestens einer Gleichung, deren Koeffizienten dem Körper $\mathfrak{k}$ angehören, nämlich der Gleichung (61); unter allen solchen Gleichungen aber wird es eine ganz bestimmte niedrig-

sten Grades geben und diese wird in $\mathfrak{k}$ irreduktibel sein; sie sei die folgende:

$$(62)\qquad x^r + k_1(\alpha)\cdot x^{r-1} + k_2(\alpha)\cdot x^{r-2} + \cdots + k_r(\alpha) = 0,$$

worin die Koeffizienten $k_i(\alpha)$, weil zu $\mathfrak{k}$ gehörig, als ganze Funktionen $n - 1^{\text{ten}}$ Grades von α mit zu $\mathfrak{R}$ gehörigen Koeffizienten gedacht werden dürfen. Hiernach besteht die Identität

$$(63)\qquad \mathsf{A}^r + k_1(\alpha)\cdot \mathsf{A}^{r-1} + k_2(\alpha)\cdot \mathsf{A}^{r-2} + \cdots + k_r(\alpha) = 0.$$

Vermittels derselben läßt sich analog mit Nr. 6 jede aus A und aus Zahlen des Bereiches $\mathfrak{k}$ rational gebildete Größe, d. i. jede Zahl ζ des Körpers K als eine ganze Funktion von A vom $r - 1^{\text{ten}}$ Grade darstellen, deren Koeffizienten zu $\mathfrak{k}$ gehören, also ganze Funktionen von α vom $n - 1^{\text{ten}}$ Grade mit zu $\mathfrak{R}$ gehörigen Koeffizienten sind. Somit hat jede Zahl ζ im Körper K die allgemeine Gestalt

$$(64)\qquad \zeta = \sum_{i,k} r_{ik}\cdot \alpha^i \mathsf{A}^k,$$

$$(i = 0, 1, 2, \cdots, n-1;\; k = 0, 1, 2, \cdots, r-1)$$

worin die r_{ik} Größen des Rationalitätsbereiches $\mathfrak{R}$ bedeuten; auch gehört jede Zahl ζ von dieser Gestalt dem Körper K an, die Formel repräsentiert daher den gesamten Körper K. Die $n\cdot r$ Größen $\alpha^i \mathsf{A}^k$ aber, durch welche hiernach jede Zahl des Körpers K linear und homogen dargestellt werden kann, sind in $\mathfrak{R}$ voneinander unabhängig, da eine Gleichung von der Gestalt

$$0 = \sum_{i,k} r_{ik}\cdot \alpha^i \mathsf{A}^k$$

auch in der Form

$$R_0(\alpha)\cdot \mathsf{A}^{r-1} + R_1(\alpha)\cdot \mathsf{A}^{r-2} + \cdots + R_{r-1}(\alpha) = 0,$$

in welcher die $R_i(\alpha)$ Größen des Bereiches $\mathfrak{k}$ wären, geschrieben werden kann und damit gegen die in $\mathfrak{k}$ stattfindende Irreduktibilität der Gleichung (62) verstieße. Hieraus folgt offenbar, daß die $n\cdot r$ Größen $\alpha^i \mathsf{A}^k$ voneinander verschieden und eine Basis des Körpers K sind, und daß dieser selbst ein in $\mathfrak{R}$ endlicher Körper vom Grade nr ist. Da r jedenfalls > 1 ist, wenn die Zahl A nicht im Körper $K(\alpha; \mathfrak{R})$ enthalten ist, so ist in dieser Voraussetzung der Grad von K größer als derjenige von $\mathfrak{k}$.

Der Körper K läßt genau $n \cdot r$ Substitutionen zu. Um dies einzusehen, bemerke man, daß eine Verwandlung des Körpers K nach den für eine Substitution geltenden Regeln auch je zwei Zahlen des in K enthaltenen Körpers $\mathfrak{k}$ nach den Formeln (53), (54) verwandeln, also auch eine Substitution des letzteren Körpers liefern wird. Demnach kann eine Substitution des Körpers K die Wurzel α nur in eine bestimmte der Wurzeln $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ verwandeln, etwa in die Wurzel α_g. Geht nun A durch dieselbe Substitution in $\mathsf{A}_h^{(g)}$ über, so geht der, der Null gleiche Ausdruck (63) in den folgenden:

$$\mathsf{A}_h^{(g)r} + k_1(\alpha_g) \cdot \mathsf{A}_h^{(g)r-1} + \cdots + k_r(\alpha_g)$$

über, der also ebenfalls Null sein muß, A verwandelt sich mithin in eine bestimmte Wurzel $\mathsf{A}_h^{(g)}$ der Gleichung

$$\text{(65)} \qquad x^r + k_1(\alpha_g)\, x^{r-1} + k_2(\alpha_g)\, x^{r-2} + \cdots + k_r(\alpha_g) = 0.$$

Sind aber diese Größen α_g, $A_h^{(g)}$ bestimmt, in welche α, A durch die Substitution übergehen, so steht zugleich die gesamte Substitution unzweideutig fest, da jede Zahl ζ wegen (64) in den völlig bestimmten Wert

$$\text{(66)} \qquad \zeta' = \sum_{i,\,k} r_{ik} \cdot \alpha_g{}^i A_h^{(g)k}$$

verwandelt werden muß. Hiernach gibt es jedenfalls nicht mehr als nr Substitutionen, da nur n Wurzeln α_g und für jede derselben nur r Wurzeln $A_h^{(g)}$ der zugehörigen Gleichung (65) vorhanden sind. Aber auch jeder dieser $n \cdot r$ Kombinationen entspricht eine Substitution des Körpers K; denn, verwandelt man die Zahlen α, A desselben in α_g, $A_h^{(g)}$ resp. und allgemeiner jede der Zahlen ζ des Körpers in die der Formel (64) entsprechend gebildete Zahl (66), so sieht man wieder, wie in voriger Nummer, leicht ein, daß dieser Verwandlung wieder der Charakter einer Substitution zukommt. Endlich sind je zwei dieser Substitutionen voneinander verschieden, da sie entweder sich in der Wurzel α_g, oder, falls diese ihnen gemeinsam wäre, doch in der zugehörigen Wurzel $A_h^{(g)}$ unterscheiden. Aus diesen Resultaten folgt aber die zu Beweis gestellte Behauptung.

11. Nun gilt der allgemeine Satz: **Sind $S_1, S_2, \cdots, S_m$ verschiedene Substitutionen eines Körpers, so enthält derselbe stets eine m-wertige Zahl,** d. h. eine solche, welche bei den m verschiedenen Substitutionen ebensoviel voneinander verschiedene Werte erhält. Dies leuchtet ein für zwei verschiedene Substitutionen, denn diese sind eben nur dann verschieden, wenn wenigstens für eine Zahl des Körpers die Werte, welche sie derselben erteilen, verschieden sind. Nehmen wir aber allgemein den Satz als bewiesen an für je $m-1$ Substitutionen, und nennen die Werte, welche eine Zahl ζ des Körpers bei den m Substitutionen $S_1, S_2, \cdots, S_m$ annimmt, $\zeta_1, \zeta_2, \cdots, \zeta_m$, so dürfen wir ζ so gewählt denken, daß etwa die $m-1$ Werte $\zeta_2, \zeta_3, \cdots, \zeta_m$ untereinander verschieden sind. Wäre dann ζ_1 nicht auch schon von diesen Werten verschieden und demnach der Satz bewiesen, so sei etwa $\zeta_1 = \zeta_2$, mithin ζ_1 von $\zeta_3, \cdots, \zeta_m$ verschieden. Wählt man nun im Körper eine Zahl η, welche durch die beiden verschiedenen Substitutionen S_1, S_2 zwei verschiedene Werte η_1, η_2 annimmt, so nimmt die, falls ϱ dem Rationalitätsbereiche entnommen wird, im Körper enthaltene Zahl

$$\xi = \varrho\zeta + \eta$$

bei den m Substitutionen die Werte an:

$$\xi_1 = \varrho\zeta_1 + \eta_1,\ \xi_2 = \varrho\zeta_2 + \eta_2, \cdots, \xi_m = \varrho\zeta_m + \eta_m,$$

sodaß der Unterschied von irgend zwei derselben

$$\xi_r - \xi_s = \varrho(\zeta_r - \zeta_s) + \eta_r - \eta_s$$

ist. Wenn hier r, s das Paar 1, 2 bedeuten, sodaß $\zeta_r = \zeta_s$ aber η_r von η_s verschieden ist, so wird auch ξ_r von ξ_s verschieden, welchen Wert ϱ auch erhalte. Für jedes andere Paar r, s der Indices ist $\zeta_r - \zeta_s$ von Null verschieden und daher gibt es in $\mathfrak{R}$ höchstens eine Zahl ϱ von der Beschaffenheit, daß $\xi_r - \xi_s$ verschwindet; nach Ausschluß dieser, den verschiedenen Paaren r, s entsprechenden, also in geringerer Anzahl als $\frac{m(m-1)}{1 \cdot 2}$ in $\mathfrak{R}$ vorhandenen Ausnahmewerte von ϱ müssen für jedes andere ϱ in $\mathfrak{R}$ die sämtlichen Werte ξ_1,

$\xi_2, \ldots, \xi_m$ verschieden voneinander sein. Somit ist der Satz, wenn er schon für $m-1$ Substitutionen gilt, auch für m Substitutionen, also, da er für zwei Substitutionen als richtig befunden worden, für jede Anzahl von solchen bewiesen.

In Verbindung desselben mit unsern vorher erhaltenen Resultaten dürfen wir nun sofort schließen, daß es im Körper K eine $n \cdot r$-wertige Zahl gibt, die nämlich bei allen den nachgewiesenen $n \cdot r$ Substitutionen des Körpers verschiedene Werte annimmt. Nun leistet aber nach Nr. 8 jede in dem in $\mathfrak{R}$ endlichen Körper $n \cdot r^{\text{ten}}$ Grades enthaltene Zahl ζ einer nur von dieser Zahl bestimmten Gleichung

$$\varphi(x) = 0$$

vom Grade $n \cdot r$ Genüge, deren Koeffizienten zu $\mathfrak{R}$ gehören. Für die gedachte Zahl ζ muß diese Gleichung in $\mathfrak{R}$ irreduktibel sein; denn, wäre

$$\varphi(x) = \psi(x)\,\chi(x),$$

wo auch die Faktoren zu $\mathfrak{R}$ gehörige Koeffizienten hätten, so müßte ζ etwa eine Wurzel von $\psi(x) = 0$ also identisch

$$\psi(\zeta) = 0$$

sein, aus welcher Gleichheit aber durch Anwendung der $n \cdot r$ Substitutionen hervorgehen würde, daß die sämtlichen $n \cdot r$ verschiedenen mit ζ konjugierten Werte die Gleichung $\psi(x) = 0$ von kleinerem Grade wie $n \cdot r$ erfüllten, was nicht sein kann.

Durch diese Betrachtungen ist also endlich festgestellt, daß im Körper K vom Grade $n \cdot r$ eine Zahl vorhanden ist, welche einer in $\mathfrak{R}$ irreduktibeln Gleichung vom Grade $n \cdot r$ Genüge leistet, also eine in $\mathfrak{R}$ algebraische Zahl $n \cdot r^{\text{ten}}$ Grades ist; heißt sie β, so werden die Potenzen

$$1, \beta, \beta^2, \cdots, \beta^{nr-1},$$

$n \cdot r$ in $\mathfrak{R}$ unabhängige Zahlen des Körpers K, also eine Basis desselben, und K nichts anderes sein, als der durch $K(\beta;\ \mathfrak{R})$ zu bezeichnende Körper.

12. Betrachten wir, nachdem wir diese Erkenntnis gewonnen, irgend einen in $\mathfrak{R}$ endlichen Körper $\mathfrak{K}$. Ist α eine

darin enthaltene Zahl, welche nach Nr. 8 als eine in $\mathfrak{R}$ algebraische Zahl etwa vom Grade n angesehen werden darf, so enthält $\mathfrak{K}$ nach der über den Rationalitätsbereich $\mathfrak{R}$ gemachten Annahme den Körper $\mathfrak{K}_1 = K(\alpha; \mathfrak{R})$ und, wenn nicht etwa $\mathfrak{K} = \mathfrak{K}_1$ ist, jedenfalls noch weiter eine Zahl A, sowie zugleich mit ihr den Körper $\mathfrak{K}_2 = K(A; \mathfrak{R})$, folglich auch den aus $\mathfrak{K}_1$, $\mathfrak{K}_2$ zusammengesetzten Körper $K(\beta; \mathfrak{R})$, dessen Grad dann ein Vielfaches von n also größer als n sein muß. Ist nun noch nicht $\mathfrak{K} = K(\beta; \mathfrak{R})$, so gibt es wieder noch weiter eine Zahl B in $\mathfrak{K}$, und man kann dasselbe Verfahren wiederholen, nämlich einen noch umfassenderen in $\mathfrak{K}$ enthaltenen Körper $K(\gamma; \mathfrak{R})$ bilden, dessen Grad wieder größer sein wird, als der von $K(\beta; \mathfrak{R})$, usw. Dieser Fortgang führt aber endlich zu einem Körper von derselben Gestalt, der mit $\mathfrak{K}$ identisch ist; denn sonst würde bei der steten Zunahme der Grade der Körper ein in $\mathfrak{K}$ enthaltener, in $\mathfrak{R}$ endlicher Körper hervorgehen, dessen Grad größer wäre als der von $\mathfrak{K}$, der also mehr in $\mathfrak{R}$ unabhängige Zahlen enthielte als $\mathfrak{K}$, was nicht sein kann. Somit sind wir zu folgendem wichtigen Satze gelangt:

Jeder in $\mathfrak{R}$ endliche Körper hat die Gestalt eines Körpers $K(A; \mathfrak{R})$, welcher durch eine in $\mathfrak{R}$ algebraische Zahl A vom Grade des Körpers erzeugt wird.

Die Gesamtheit seiner Zahlen ζ wird daher nach Nr. 6 durch die Formel

$$\zeta = r_0 + r_1 A + r_2 A^2 + \cdots + r_{N-1} A^{N-1}$$

repräsentiert, wenn N den Grad des Körpers und die Koeffizienten r_i sämtliche Zahlen des Rationalitätsbereiches bedeuten; sind ferner

$$A,\ A^{(1)},\ A^{(2)}, \cdots, A^{(N-1)}$$

die Wurzeln der irreduktibeln Gleichung $F(x) = 0$ vom N^{ten} Grade, der A Genüge leistet, so erhält man die zu $K(A; \mathfrak{R})$ konjugierten Körper, bezw. die zu ζ konjugierten Zahlen

$$\zeta,\ \zeta^{(1)},\ \zeta^{(2)}, \cdots, \zeta^{(N-1)},$$

rindem man in der obigen Formel A durch alle jene Wurzeln esp. ersetzt.

Irgend ein Unterkörper des in $\mathfrak{R}$ endlichen Körpers $\mathfrak{K}$ ist offenbar wieder ein in $\mathfrak{R}$ endlicher Körper, denn, während jede

Zahl desselben für sich unabhängig ist, kann er nicht mehr als soviel in $\mathfrak{R}$ unabhängige Zahlen enthalten, als sich in $\mathfrak{K}$ selbst finden, demnach wird eine gewisse Anzahl m solcher unabhängiger Zahlen im Unterkörper vorhanden sein, während zwischen je $m+1$ Zahlen desselben eine lineare Beziehung mit zu $\mathfrak{R}$ gehörigen Koeffizienten besteht. Hieraus schließt man, daß jeder Unterkörper von $\mathfrak{K}$ wieder die Gestalt $K(\alpha; \mathfrak{R})$ haben, nämlich durch eine in $\mathfrak{K}$ enthaltene Zahl α erzeugt werden muß. Da umgekehrt der durch irgend eine solche Zahl α erzeugte Körper $K(\alpha; \mathfrak{R})$ ein Unterkörper von $\mathfrak{K}$ sein wird, so stimmt die Gesamtheit der Unterkörper von $\mathfrak{K}$ mit den durch sämtliche in $\mathfrak{K}$ enthaltenen Zahlen α erzeugten Körpern $K(\alpha; \mathfrak{R})$ und ihr jedesmaliger Grad mit dem in Nr. 6 definierten Grade der erzeugenden Zahl α überein.

13. Wenn aber in Nr. 10 der Körper $K(\alpha; \mathfrak{R})$ als ein Teiler des Körpers $K(A; \mathfrak{R})$ gedacht wird, so wird der dort betrachtete, aus beiden zusammengesetzte Körper mit dem letzteren identisch sein (s. (11)), und es ergibt sich die Gleichung

$$N = n \cdot r.$$

Da hiernach n ein Teiler von N ist, so ist der Grad jedes Unterkörpers eines endlichen Körpers, sowie der Grad jeder in letzterem enthaltenen Zahl ein Teiler vom Grade dieses Körpers.

Verstehen wir daher unter $K(A; \mathfrak{R})$ einen endlichen Körper von einem Grade, den wir N nennen, und unter $K(\alpha; \mathfrak{R})$ den von irgend einer in ihm enthaltenen Zahl α erzeugten Unterkörper n^{ten} Grades, so wird zunächst $N = n \cdot r$ oder der Grad der im Rationalitätsbereiche $K(\alpha; \mathfrak{R})$ irreduktibeln Gleichung

$$x^r + k_1(\alpha) \cdot x^{r-1} + k_2(\alpha) \cdot x^{r-2} + \cdots + k_r(\alpha) = 0, \tag{67}$$

welcher die Zahl A genügt,

$$r = \frac{N}{n} \tag{68}$$

sein. Ferner aber erhält man in den $N = n \cdot r$ Zahlen

$$\alpha^i \cdot A^k \tag{69}$$
$$(i = 0, 1, 2, \cdots, n-1;\ k = 0, 1, 2, \cdots, r-1)$$

eine Basis des Körpers $K(A; \mathfrak{R})$. Benutzt man diese nun zur Ermittlung der charakteristischen Gleichung N^{ten} Grades für die Zahl α, wie sie in Nr. 8 hergeleitet worden ist, indem man die folgenden N mit (32) analogen Gleichungen aufstellt:

$$
\begin{aligned}
&(\alpha - \varrho) \cdot 1 = -\varrho \cdot 1 + 1 \cdot \alpha, \\
&(\alpha - \varrho) \cdot \alpha = \qquad -\varrho \cdot \alpha + 1 \cdot \alpha^2, \\
&\cdots\cdots\cdots\cdots \\
&(\alpha - \varrho) \cdot \alpha^{n-1} = -a_n \cdot 1 - a_{n-1} \cdot \alpha - a_{n-2} \cdot \alpha^2 - \cdots - (\varrho + a_1) \cdot \alpha^{n-1}, \\
&(\alpha - \varrho) \cdot A = -\varrho A + 1 \cdot \alpha A, \\
&(\alpha - \varrho) \cdot \alpha A = \qquad -\varrho \cdot \alpha A + 1 \cdot \alpha^2 A, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&(\alpha - \varrho) \cdot \alpha^{n-1} A = -a_n \cdot A - a_{n-1} \cdot \alpha A - a_{n-2} \cdot \alpha^2 A - \cdots \\
&\qquad\qquad - (\varrho + a_1) \cdot \alpha^{n-1} A, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&(\alpha - \varrho) \cdot A^{r-1} = -\varrho \cdot A^{r-1} + 1 \cdot \alpha A^{r-1}, \\
&(\alpha - \varrho) \cdot \alpha A^{r-1} = \qquad -\varrho \cdot \alpha A^{r-1} + 1 \cdot \alpha^2 A^{r-1}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&(\alpha - \varrho) \cdot \alpha^{n-1} A^{r-1} = -a_n \cdot A^{r-1} - a_{n-1} \cdot \alpha A^{r-1} - a_{n-2} \cdot \alpha^2 A^{r-1} \\
&\qquad\qquad - \cdots - (\varrho + a_1) \cdot \alpha^{n-1} A^{r-1},
\end{aligned}
$$

in denen unter ϱ irgend eine Größe des Rationalitätsbereiches $\mathfrak{R}$ verstanden ist, so lassen diese Gleichungen mit Beachtung der in der Formel (38) gegebenen Definition der Norm ohne weiteres erkennen, daß die Norm von $\alpha - \varrho$ gleich

$$
\begin{vmatrix}
-\varrho, & 1, & 0, & 0, \cdots\cdots, & 0, \\
0, & -\varrho, & 1, & 0, \cdots\cdots, & 0, \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
-a_n, & -a_{n-1}, & -a_{n-2}, & -a_{n-3}, \cdots, & -(\varrho + a_1)
\end{vmatrix}^r
$$

ist, oder daß, wenn wieder mit

$$\varphi(x) = 0$$

die Gleichung N^{ten} Grades bezeichnet wird, welche

für die Zahl α charakteristisch ist, nach (46) — wo n durch $N = nr$ zu ersetzen ist —

$$\varphi(\varrho) = \begin{vmatrix} \varrho, & -1, & 0, \cdots\cdots, & 0, \\ 0, & \varrho, & -1, \cdots\cdots, & 0, \\ \cdot & \cdot & \cdot & \cdot \\ a_n, & a_{n-1}, & a_{n-2}, \cdots, & \varrho + a_1 \end{vmatrix}^r$$

ist. Da aber diese algebraische Gleichung für die unendlich vielen in $\Re$ enthaltenen Zahlen ϱ erfüllt ist, besteht sie identisch, und somit ist die ganze Funktion $\varphi(x)$ vom Grade $N = nr$ die r^{te} Potenz einer anderen ganzen Funktion n^{ten} Grades von x, deren Koeffizienten zu $\Re$ gehören, und welcher die Zahl α genügen muß. Letztere Funktion kann daher keine andere sein, als die in $\Re$ irreduktible, diese Zahl α definierende Funktion

$$(70) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n,$$

deren Wurzeln, entsprechend mit Nr. 10, $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ zu nennen sein würden.

Bemerkt man einerseits, daß bei den N Substitutionen des Körpers $K(A; \Re)$ die Zahlen α, A in die N Wertepaare $\alpha_g, A_h^{(g)}$, die Zahl α also r Mal in jede der Wurzeln $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ übergeht, daß aber andererseits diese r-fach genommenen Werte sämtliche Wurzeln der charakteristischen Gleichung $\varphi(x) = 0$ sind, so erkennt man, daß die den N Substitutionen zugehörigen konjugierten Werte von α mit den sämtlichen (gleichen oder ungleichen) Wurzeln der letzteren Gleichung übereinstimmen, derart, daß man setzen darf

$$(71) \quad \varphi(x) = (x - \alpha)(x - \alpha^{(1)})(x - \alpha^{(2)}) \cdots (x - \alpha^{(N-1)});$$

und so gewinnt man eine neue Definition der Spur wie der Norm einer Zahl α des endlichen Körpers:

Die *Spur* $S(\alpha)$ ist die *Summe*, und die *Norm* $N(\alpha)$ ist das *Produkt* aller N konjugierten Werte von α.

14. Setzt man analog mit Nr. 8

$$\varphi(x) = x^N + R_1 x^{N-1} + R_2 x^{N-2} + \cdots + R_N,$$

so ist

$$\varphi'(\alpha) = N \cdot \alpha^{N-1} + (N-1) R_1 \cdot \alpha^{N-2} + \cdots + 1 \cdot R_{N-1}$$

eine zugleich mit α im Körper $K(A; \mathfrak{R})$ enthaltene Zahl, die auch zugleich mit α völlig bestimmt ist. Sie soll durch eine besondere Benennung als die *Differente* von α und mit dem Zeichen $\partial(\alpha)$ ausgezeichnet werden. Da man bekanntlich auch

$$\varphi'(\alpha) = (\alpha - \alpha^{(1)})(\alpha - \alpha^{(2)}) \cdots (\alpha - \alpha^{(N-1)})$$

und gleicherweise

$$\varphi'(\alpha^{(1)}) = (\alpha^{(1)} - \alpha)(\alpha^{(1)} - \alpha^{(2)}) \cdots (\alpha^{(1)} - \alpha^{(N-1)})$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\varphi'(\alpha^{(N-1)}) = (\alpha^{(N-1)} - \alpha)(\alpha^{(N-1)} - \alpha^{(2)}) \cdots (\alpha^{(N-1)} - \alpha^{(N-2)})$$

setzen kann, ergibt sich gemäß der neuen Bedeutung der Norm die Beziehung

$$N\partial(\alpha) = (-1)^{\frac{N(N-1)}{2}} \cdot \prod (\alpha^{(i)} - \alpha^{(k)})^2, \tag{72}$$

wo die Multiplikation auf alle Werte i, k aus der Reihe $0, 1, 2, \cdots, N-1$ zu erstrecken ist, bei denen $i < k$. Nach bekanntem Determinantensatze ist das Produkt

$$\prod (\alpha^{(i)} - \alpha^{(k)}) = \begin{vmatrix} 1, & \alpha, & \alpha^2, & \cdots\cdots & \alpha^{N-1} \\ 1, & \alpha^{(1)}, & \alpha^{(1)2} & \cdots\cdots & \alpha^{(1)\,N-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1, & \alpha^{(N-1)}, & \alpha^{(N-1)2} & \cdots & \alpha^{(N-1)\,N-1} \end{vmatrix}, \tag{73}$$

d. i. gleich einer Determinante, deren Quadrat die Diskriminante der *Gleichung* $\varphi(x) = 0$ genannt zu werden pflegt und deshalb auch als Diskriminante der *Zahl* α bezeichnet werden soll. Schreibt man dafür kurz $\Delta(\alpha)$, so ergibt sich zwischen Differente und Diskriminante einer Zahl die Beziehung

$$N\partial(\alpha) = (-1)^{\frac{N\cdot(N-1)}{2}} \cdot \Delta(\alpha), \tag{74}$$

und aus diesen Formeln die Tatsache, daß eine Zahl α dann

und nur dann eine N-wertige Zahl ist, wenn ihre Diskriminante (oder Differente; denn mit der Norm $N\partial(\alpha)$ ist immer zugleich auch $\partial(\alpha)$ Null oder zugleich von Null verschieden) von Null verschieden ist. Eine N-wertige Zahl ist aber stets N^{ten} Grades, nämlich die ihr charakteristische Gleichung $\varphi(x) = 0$ irreduktibel (s. Nr. 11), während für eine Zahl, die minderwertig ist, diese Gleichung gleiche Wurzeln haben also reduktibel, mithin der Grad von α geringer als N sein würde; im ersteren und nur im ersteren Falle bilden die Potenzen $1, \alpha, \alpha^2, \cdots, \alpha^{N-1}$ eine Basis des Körpers $K(A; \mathfrak{R})$ und ist mithin α eine ihn erzeugende Zahl. Man darf daher das vorige Resultat auch so aussprechen:

Je nachdem die Diskriminante (oder Differente) einer Zahl α des Körpers $K(A; \mathfrak{R})$ von Null verschieden ist oder nicht, ist α eine den Körper erzeugende Zahl oder nicht.

Die Gesamtheit aller den Körper N^{ten} Grades erzeugenden Zahlen hat die charakteristische Eigenschaft, daß je zwei von ihnen mittels des Rationalitätsbereiches rational durch einander ausdrückbar sind. Eine solche Gesamtheit nennt Kronecker eine Gattung $\mathfrak{G}$ von N^{ter} Ordnung. Der durch jede beliebige ihrer Zahlen gleicherweise erzeugte Körper N^{ten} Grades heißt dann der zur Gattung $\mathfrak{G}$ gehörige Gattungsbereich.

Nun seien

$$\zeta_1, \zeta_2, \cdots, \zeta_N$$

N verschiedene Zahlen des Körpers und Z die nachstehende, aus diesen Zahlen und ihren Konjugierten gebildete Determinante:

$$(75) \qquad Z = \begin{vmatrix} \zeta_1, & \zeta_2, & \cdots\cdots\cdots, & \zeta_N, \\ \zeta_1^{(1)}, & \zeta_2^{(1)}, & \cdots\cdots\cdots, & \zeta_N^{(1)}, \\ \cdot & \cdot & \cdot\;\cdot\;\cdot\;\cdot & \cdot \\ \zeta_1^{(N-1)}, & \zeta_2^{(N-1)}, & \cdots, & \zeta_N^{(N-1)} \end{vmatrix}.$$

Für das Quadrat dieser Determinante findet sich, wenn bei der Multiplikation Kolonnen mit Kolonnen verbunden werden, mit

Beachtung der neuen Bedeutung der Spur einer Zahl die folgende Determinante:

$$Z^2 = \begin{vmatrix} S(\zeta_1\zeta_1), & S(\zeta_1\zeta_2), & \cdots, & S(\zeta_1\zeta_N), \\ S(\zeta_2\zeta_1), & S(\zeta_2\zeta_2), & \cdots, & S(\zeta_2\zeta_N), \\ \cdot & \cdot & \cdot & \cdot \\ S(\zeta_N\zeta_1), & S(\zeta_N\zeta_2), & \cdots, & S(\zeta_N\zeta_N) \end{vmatrix},$$

d. h. (siehe (49), (50)) die Gleichung

$$(76) \qquad Z^2 = \Delta(\zeta_1, \zeta_2, \cdots, \zeta_N),$$

oder der Satz: **Das Quadrat der Determinante Z ist die Diskriminante der N Zahlen $\zeta_1, \zeta_2, \cdots, \zeta_N$ und demnach bilden diese Zahlen eine Basis des Körpers $K(A; \mathfrak{R})$ oder nicht, jenachdem die Determinante Z von Null verschieden ist oder nicht.**

Insbesondere geht, wenn

$$(77) \qquad \zeta_1 = 1, \; \zeta_2 = \alpha, \; \zeta_3 = \alpha^2, \; \cdots, \; \zeta_N = \alpha^{N-1}$$

gewählt werden, die Determinante Z über in die in Gleichung (73) enthaltene Determinante, und somit ist die Diskriminante $\Delta(\alpha)$ der Zahl α nichts anderes, als die Diskriminante $\Delta(1, \alpha, \alpha^2, \cdots, \alpha^{N-1})$ **des Systems der Zahlen** $1, \alpha, \alpha^2, \cdots, \alpha^{N-1}$.

15. **Daher ist die Diskriminante der den Körper $K(A; \mathfrak{R})$ erzeugenden Zahl A zugleich die Diskriminante seiner Basis** $1, A, A^2, \cdots, A^{N-1}$. Zufolge der allgemeineren Formel (51) unterscheidet sich von der letzteren die Diskriminante irgend einer anderen Basis des Körpers nur um einen quadratischen, in $\mathfrak{R}$ enthaltenen Faktor. Wir betrachten hier insbesondere noch diejenige, Nr. 13 entsprechende Basis des Körpers, welche aus den Zahlen

$$\alpha^i \cdot A^k$$
$$(i = 0, 1, 2, \cdots, n-1; \; k = 0, 1, 2, \cdots, r-1),$$

besteht und bilden ihre Diskriminante. Diese ist das Quadrat nachstehender Determinante:

$$(78)\qquad \left|\begin{array}{l}
1,\ \alpha,\ \cdots\cdots,\ \alpha^{n-1},\ A,\quad \alpha A,\ \cdots\cdots\cdots\cdots,\quad \alpha^{n-1}A,\ \cdots \\
\qquad\qquad\qquad\qquad\qquad A^{r-1},\ \alpha A^{r-1},\ \cdots,\ \alpha^{n-1}A^{r-1} \\
1,\ \alpha,\ \cdots\cdots,\ \alpha^{n-1},\ A_1,\quad \alpha A_1,\ \cdots\cdots\cdots\cdots,\quad \alpha^{n-1}A_1,\ \cdots \\
\qquad\qquad\qquad\qquad\qquad A_1^{r-1},\ \alpha A_1^{r-1},\ \cdots,\ \alpha^{n-1}A_1^{r-1} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
1,\ \alpha,\ \cdots\cdots,\ \alpha^{n-1},\ A_{r-1},\ \alpha A_{r-1},\ \cdots\cdots\cdots,\quad \alpha^{n-1}A_{r-1},\ \cdots \\
\qquad\qquad\qquad\qquad\qquad A_{r-1}^{r-1},\ \alpha A_{r-1}^{r-1},\ \cdots,\ \alpha^{n-1}A_{r-1}^{r-1} \\
1,\ \alpha_1,\ \cdots\cdots,\ \alpha_1^{n-1},\ A^{(1)},\quad \alpha_1 A^{(1)},\ \cdots\cdots\cdots\cdots,\ \alpha_1^{n-1}A^{(1)},\ \cdots \\
\qquad\qquad\qquad\qquad\qquad A^{(1)r-1},\ \alpha_1 A^{(1)r-1},\ \cdots,\ \alpha_1^{n-1}A^{(1)r-1} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
1,\ \alpha_{n-1},\ \cdots,\ \alpha_{n-1}^{n-1},\ A^{(n-1)},\ \alpha_{n-1}A^{(n-1)},\ \cdots,\ \alpha_{n-1}^{n-1}A^{(n-1)},\ \cdots \\
\qquad\qquad\qquad A^{(n-1)r-1},\ \alpha_{n-1}A^{(n-1)r-1},\ \cdots,\ \alpha_{n-1}^{n-1}A^{(n-1)r-1} \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
1,\ \alpha_{n-1},\ \cdots,\ \alpha_{n-1}^{n-1},\ A_{r-1}^{(n-1)},\ \alpha_{n-1}A_{r-1}^{(n-1)},\ \cdots,\ \alpha_{n-1}^{n-1}A_{r-1}^{(n-1)},\ \cdots \\
\qquad\qquad\qquad\qquad\qquad A_{r-1}^{(n-1)r-1},\ \cdots,\ \alpha_{n-1}^{n-1}A_{r-1}^{(n-1)r-1}
\end{array}\right|,$$

in welcher für einen Augenblick mit $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ wieder die Wurzeln der in $\mathfrak{R}$ irreduktibeln Gleichung

$$(79)\qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0,$$

welcher die Zahl α genügt, und mit

$$A^{(i)},\ A_1^{(i)},\ \cdots,\ A_{r-1}^{(i)},$$

die Wurzeln der im Körper $K(\alpha_i;\ \mathfrak{R})$ irreduktibeln, mit (67) konjugierten Gleichung

$$(80)\qquad x^r + k_1(\alpha_i)\cdot x^{r-1} + k_2(\alpha_i)\cdot x^{r-2} + k_r(\alpha_i) = 0$$

bezeichnet worden sind. Nach den Regeln der Determinantentheorie ist die Determinante (78) das Produkt folgender Faktoren:

$$(81)\qquad \left\{\begin{array}{l}
\qquad\qquad\qquad \left|\begin{array}{llll}
1, \alpha, & \alpha^2, & \cdots, & \alpha^{n-1} \\
1, \alpha_1, & \alpha_1^2, & \cdots, & \alpha_1^{n-1} \\
\cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\
1, \alpha_{n-1}, & \alpha_{n-1}^2, & \cdots, & \alpha_{n-1}^{n-1}
\end{array}\right|^r, \\
\left|\begin{array}{llll}
1, A, & A^2, & \cdots, & A^{r-1} \\
1, A_1, & A_1^2, & \cdots, & A_1^{r-1} \\
\cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\
1, A_{r-1}, & A_{r-1}^2, & \cdots, & A_{r-1}^{r-1}
\end{array}\right|, \cdots, \left|\begin{array}{lll}
1, A^{(n-1)}, & \cdots, & A^{(n-1)r-1} \\
1, A_1^{(n-1)}, & \cdots, & A_1^{(n-1)r-1} \\
\cdot\ \cdot & \cdot\ \cdot & \cdot\ \cdot \\
1, A_{r-1}^{(n-1)}, & \cdots, & A_{r-1}^{(n-1)r-1}
\end{array}\right|.
\end{array}\right.$$

Das Quadrat der ersten dieser Determinanten ist aber die Diskriminante der Gleichung (79), d. i. die Diskriminante der Zahl α, wenn diese als dem Körper $\mathfrak{k} = K(\alpha; \mathfrak{R})$ angehörig gedacht, ihre Diskriminante nämlich in diesem Körper gebildet wird; wir bezeichnen sie als solche mit $\delta(\alpha)$, sowie die im Körper $\mathfrak{K} = K(A; \mathfrak{R})$ vom Grade N gebildete Diskriminante der Zahlen $\alpha^i A^k$ mit $\Delta(\cdots, \alpha^i A^k, \cdots)$; beide sind, da sie rational aus Spuren zusammengesetzt sind (vgl. Nr. 8), im Rationalitätsbereiche $\mathfrak{R}$ enthaltene Größen. Denkt man sich andererseits den aus A und $\mathfrak{R}$ hervorgehenden Körper $\mathfrak{K}$, wie oben, aus der Wurzel A der in $\mathfrak{k}$ irreduktibeln Gleichung (67) und dem Rationalitätsbereiche $\mathfrak{k}$ entstanden und bezeichnet ihn entsprechend durch $\mathfrak{K} = K(A; \mathfrak{k})$, so ist das Quadrat der zweiten der Determinanten (81) offenbar die Diskriminante der Gleichung (67), d. h. die Diskriminante der Zahl A, wenn diese als eine Zahl des Körpers $K(A; \mathfrak{k})$ vom Grade r aufgefaßt, ihre Diskriminante also in diesem Körper mit dem Rationalitätsbereiche $\mathfrak{k}$ gebildet wird; als solche wird sie eine im letztern enthaltene Zahl sein, und ihre konjugierten Werte erhalten werden, wenn α durch die anderen Werte $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ der den Körper $\mathfrak{k}$ erzeugenden Zahl α ersetzt wird, wodurch allgemein A_i in $A_i^{(1)}, A_i^{(2)}, \cdots, A_i^{(n-1)}$ resp., die zweite der Determinanten (81) also in die folgenden verwandelt wird. Bezeichnet man daher die in der angegebenen Weise mit Bezug auf den Rationalitätsbereich $\mathfrak{k}$ gebildete Diskriminante, die sogenannte R e l a t i v d i s k r i m i n a n t e der Zahl A mit $\Delta_{\mathfrak{k}}(A)$, so wird das Produkt aus den Quadraten der letztbetrachteten n Determinanten nichts anderes sein, als die in $\mathfrak{k}$ genommene Norm dieser Größe, welche durch $n(\Delta_{\mathfrak{k}}(A))$ bezeichnet werden mag. S o g e l a n g t m a n s c h l i e ß l i c h z u d e r f o l g e n d e n w i c h t i g e n B e z i e h u n g:

$$\Delta(\cdots, \alpha^i A^k, \cdots) = \delta(\alpha)^r \cdot n(\Delta_{\mathfrak{k}}(A)), \tag{82}$$

a u f d i e s p ä t e r z u r ü c k g e w i e s e n w e r d e n w i r d.

16. Bilden die N Zahlen $\omega_1, \omega_2, \cdots, \omega_N$ irgend eine Basis des Körpers N^{ten} Grades, so ist die Determinante

$$\begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2), & \cdots, & S(\omega_1\omega_N), \\ S(\omega_2\omega_1), & S(\omega_2\omega_2), & \cdots, & S(\omega_2\omega_N), \\ \cdot & \cdot & \cdot & \cdot \\ S(\omega_N\omega_1), & S(\omega_N\omega_2), & \cdots, & S(\omega_N\omega_N) \end{vmatrix}$$

als Diskriminante der Basis von Null verschieden. Durch Auflösung des Systems linearer Gleichungen

$$(83)\quad \omega_i = S(\omega_i\omega_1)\cdot\omega_1' + S(\omega_i\omega_2)\cdot\omega_2' + \cdots + S(\omega_i\omega_N)\cdot\omega_N' \qquad (i = 1, 2, \cdots, N)$$

ergibt sich daher ein bestimmtes endliches Wertsystem ω_1', ω_2', $\cdots$, ω_N', dessen Glieder, weil die sämtlichen Koeffizienten $S(\omega_i\omega_k)$ als Spuren von Zahlen des Körpers zu $\Re$ gehören, mit $\omega_1, \omega_2, \cdots, \omega_N$ zugleich Zahlen des Körpers und ebenfalls eine Basis desselben bilden, da durch sie die letztgenannten und folglich alle Zahlen des Körpers linear ausdrückbar sind. Diese neue Basis des Körpers soll die zur ersteren komplementäre Basis heißen.

Sei nun

$$\zeta = \rho_1\omega_1 + \rho_2\omega_2 + \cdots + \rho_N\omega_N$$

eine beliebige Zahl des Körpers, so folgt mit Rücksicht auf die in den Formeln (41), (42) ausgedrückten Eigenschaften der Spur aus (83) die Gleichung

$$(84)\quad \zeta = S(\zeta\omega_1)\cdot\omega_1' + S(\zeta\omega_2)\cdot\omega_2' + \cdots + S(\zeta\omega_N)\cdot\omega_N',$$

welche jene als speziellen Fall in sich enthält; für den besonderen Wert $\zeta = \omega_i'$ aber liefert sie wegen der in $\Re$ stattfindenden Unabhängigkeit der Zahlen $\omega_1', \omega_2', \cdots, \omega_N'$ sogleich die Beziehung

$$(85)\quad S(\omega_i'\omega_k) = (i, k),$$

wo unter dem Symbole (i, k) die Eins oder die Null verstanden wird, je nachdem i, k einander gleich oder voneinander verschieden sind. Bedeuten daher Ω, Ω' die Werte der Determinante Z, wenn darin unter $\zeta_1, \zeta_2, \cdots, \zeta_N$ einmal die Zahlen $\omega_1, \omega_2, \cdots, \omega_N$, das andere Mal die Zahlen $\omega_1', \omega_2', \cdots, \omega_N'$ gedacht werden, so folgt aus (85) für das Produkt derselben, d. h. für den Ausdruck

$$\Omega\cdot\Omega' = \begin{vmatrix} S(\omega_1'\omega_1), & S(\omega_1'\omega_2), & \cdots, & S(\omega_1'\omega_N) \\ S(\omega_2'\omega_1), & S(\omega_2'\omega_2), & \cdots, & S(\omega_2'\omega_N) \\ \cdot & \cdot & \cdot & \cdot \\ S(\omega_N'\omega_1), & S(\omega_N'\omega_2), & \cdots, & S(\omega_N'\omega_N) \end{vmatrix}$$

die Gleichung

$$(86)\quad \Omega\cdot\Omega' = 1$$

und folglich auch

$$(87)\qquad \Delta(\omega_1, \omega_2, \cdots, \omega_N)\cdot\Delta(\omega_1', \omega_2', \cdots, \omega_N') = 1.$$

Die so für eine Basis $\omega_1, \omega_2, \cdots, \omega_N$ und für ihre komplementäre Basis $\omega_1', \omega_2', \cdots, \omega_N'$ gefundene Beziehung (85) reicht nun auch hin, zwei ihr genügende Systeme von Zahlen des Körpers als zu einander komplementäre Basen desselben erkennen zu lassen und ist demnach charakteristisch für solche. Denn, wenn für zwei Systeme ω_i, ω_i' von Zahlen des Körpers die Beziehung (85) besteht, so bildet zunächst jedes derselben, da aus (85) sich (87) ergibt, ihre Diskriminanten also nicht verschwinden, eine Basis des Körpers, sodaß man Gleichungen ansetzen kann von der Form

$$(88)\qquad \omega_i = a_{i1}\omega_1' + a_{i2}\omega_2' + \cdots + a_{iN}\omega_N', \quad (i = 1, 2, \cdots, N)$$

in denen die Koeffizienten a_{ik} in $\mathfrak{R}$ enthalten sind; aus diesen aber folgt

$$S(\omega_i\omega_k) = a_{i1}\cdot S(\omega_1'\omega_k) + a_{i2}\cdot S(\omega_2'\omega_k) + \cdots + a_{iN}\cdot S(\omega_N'\omega_k),$$

d. i. wegen (85)

$$a_{ik} = S(\omega_i\omega_k),$$

mithin stimmen die Gleichungen (88) mit den Gleichungen (83) überein und ergeben so $\omega_1', \omega_2', \cdots, \omega_N'$ als die zu $\omega_1, \omega_2, \cdots, \omega_N$ komplementäre Basis. Da aber die Beziehungen (85) vollkommen symmetrisch sind in bezug auf die beiden Zahlensysteme, so findet sich ebenso $\omega_1, \omega_2, \cdots, \omega_N$ als die zu $\omega_1', \omega_2', \cdots, \omega_N'$ komplementäre Basis; die mit diesem Ausdruck bezeichnete Beziehung zwischen zwei Zahlensystemen des Körpers findet mithin stets gegenseitig statt.

Wie die Gleichung (85) ist übrigens auch die Gleichung (84) für zwei komplementäre Basen charakteristisch: zwei Systeme $\omega_1, \omega_2, \cdots, \omega_N$ und $\omega_1', \omega_2', \cdots, \omega_N'$ sind solche Basen, wenn jene Gleichung für jede Zahl ζ des Körpers besteht. Denn jedenfalls muß alsdann das zweite der Systeme eine Basis des Körpers sein; da aber dann für $\zeta = \omega_i'$ sich aus jener Gleichung die Beziehung (85) ergibt, so ist auch das erste System eine Basis des Körpers, nämlich die zum vorigen komplementäre.

Nach der kurz voraufgehenden Aussage darf man in der Gleichung (84) die beiden Basen miteinander vertauschen, sodaß für jede Zahl ζ des Körpers auch die folgende Beziehung erfüllt ist:

$$(89) \quad \zeta = S(\zeta\omega_1') \cdot \omega_1 + S(\zeta\omega_2') \cdot \omega_2 + \cdots + S(\zeta\omega_N') \cdot \omega_N.$$

Insbesondere bestehen also neben den Gleichungen (83) die nachstehenden, welche ihre Auflösung repräsentieren:

$$(90) \quad \omega_i' = S(\omega_i'\omega_1') \cdot \omega_1 + S(\omega_i'\omega_2') \cdot \omega_2 + \cdots + S(\omega_i'\omega_N') \cdot \omega_N.$$

Durch Substitution der Werte (83) ergibt sich aus ihnen

$$\omega_i' = \sum_h \left(\omega_h' \cdot \sum_k S(\omega_h\omega_k)\, S(\omega_i'\omega_k')\right)$$

und folglich wegen der Unabhängigkeit der ω_i' untereinander **die Gleichheit**

$$(91) \qquad \sum_k S(\omega_h\omega_k)\, S(\omega_i'\omega_k') = (i,\ h).$$

Wenn nun $\zeta_1, \zeta_2, \cdots, \zeta_N$ irgend eine andere Basis des Körpers bedeuten, welche mit der Basis $\omega_1, \omega_2, \cdots, \omega_N$ durch N lineare Gleichungen

$$(92) \qquad \zeta_i = \varrho_{i1}\omega_1 + \varrho_{i2}\omega_2 + \cdots + \varrho_{iN}\omega_N \quad (i = 1, 2, \cdots, N)$$

verbunden ist, so ergibt sich durch Vergleichung mit (89) für alle i, k die Gleichheit

$$\varrho_{ik} = S(\zeta_i\omega_k').$$

Ist aber $\zeta_1', \zeta_2', \cdots, \zeta_N'$ die zu $\zeta_1, \zeta_2, \cdots, \zeta_N$ komplementäre Basis, so liefert die bezügliche, mit (84) analoge Formel für $\zeta = \omega_i'$ die Gleichung

$$\omega_i' = S(\omega_i'\zeta_1) \cdot \zeta_1' + S(\omega_i'\zeta_2) \cdot \zeta_2' + \cdots + S(\omega_i'\zeta_N) \cdot \zeta_N'$$

d. h.

$$(93) \qquad \omega_i' = \varrho_{1i}\zeta_1' + \varrho_{2i}\zeta_2' + \cdots + \varrho_{Ni}\zeta_N' \quad (i = 1, 2, \cdots, N)$$

d. h. den Satz: **Bestehen zwischen den beiden Basen $\zeta_1, \zeta_2, \cdots, \zeta_N$ und $\omega_1, \omega_2, \cdots, \omega_N$ die Gleichungen (92), so gelten zwischen den zu ihnen resp. komplementären Basen $\zeta_1', \zeta_2', \cdots, \zeta_N'$ und $\omega_1', \omega_2', \cdots, \omega_N'$ die „transponierten" Gleichungen (93).**

Ersetzt man ζ in (89) durch $\zeta\omega_i$, so kommt

$$\zeta\omega_i = S(\zeta\omega_i\omega_1') \cdot \omega_1 + S(\zeta\omega_i\omega_2') \cdot \omega_2 + \cdots + S(\zeta\omega_i\omega_N') \quad \omega_N$$
$$(i = 1, 2, \cdots N).$$

Die Vergleichung dieses Systems von Gleichungen mit den Gleichungen (32) und die Definition (39) für die Spur einer Zahl läßt sogleich erkennen, daß

$$S(\zeta) = S(\zeta\omega_1\omega_1') + S(\zeta\omega_2\omega_2') + \cdots + S(\zeta\omega_N\omega_N'),$$

d. h.

$$(94) \qquad S(\zeta) = S(\zeta\sigma)$$

ist, wenn man zur Abkürzung

$$(95) \qquad \sigma = \omega_1\omega_1' + \omega_2\omega_2' + \cdots + \omega_N\omega_N'$$

setzt. Gemäß dieser für jede Zahl ζ des Körpers gefundenen Beziehung nimmt die Formel (89) für $\zeta = \sigma$ die Gestalt an:

$$\sigma = S(\omega_1')\,\omega_1 + S(\omega_2')\,\omega_2 + \cdots + S(\omega_N')\,\omega_N,$$

ein Ausdruck, der aus ihr auch für $\zeta = 1$ hervorgeht, und somit ist σ, d. h.

$$(96) \qquad \omega_1\omega_1' + \omega_2\omega_2' + \cdots \omega_N\omega_N' = 1.$$

Da nun aus (83)

$$\sum_{i,k} S(\omega_i'\omega_k')\,\omega_i\omega_k = \sum_{h,i,k} S(\omega_i\omega_h)\,S(\omega_i'\omega_k')\,\omega_k\omega_h'$$

und aus (90)

$$\sum_{i,k} S(\omega_i\omega_k)\,\omega_i'\omega_k' = \sum_{h,i,k} S(\omega_i\omega_k)\,S(\omega_i'\omega_h')\,\omega_h\omega_k'$$

hervorgeht, so findet sich mit Beachtung von (91) jede dieser beiden Summen gleich

$$\omega_1\omega_1' + \omega_2\omega_2' + \cdots + \omega_N\omega_N'$$

und wegen (96) also noch nachstehende Doppelgleichheit:

$$\sum_{i,k} S(\omega_i'\omega_k')\,\omega_i\omega_k = \sum_{i,k} S(\omega_i\omega_k)\,\omega_i'\omega_k' = 1.$$

17. Zum Beschluß dieser allgemeinen Betrachtungen über Zahlenkörper denken wir uns noch den (nach Nr. 11 und 12 endlichen) Körper $\mathfrak{K} = K(A; \mathfrak{R})$ vom Grade N, welcher aus dem endlichen Körper $\mathfrak{k} = K(\alpha; \mathfrak{R})$ vom n^{ten} Grade und allen ihm konjugierten Körpern $\mathfrak{k}^{(1)}, \mathfrak{k}^{(2)}, \cdots, \mathfrak{k}^{(n-1)}$ zusammengesetzt ist.

Die bezüglich $\mathfrak{k}$ zu einander konjugierten Zahlen α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots, \alpha^{(n-1)}$ sind die Wurzeln einer in $\mathfrak{R}$ irreduktibeln Gleichung, welche wieder

$$(97) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

heiße; jede in $\mathfrak{K}$ enthaltene Zahl ist mithin aus α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots, \alpha^{(n-1)}$ und Zahlen des Rationalitätsbereiches $\mathfrak{R}$ in rationaler Weise zusammengesetzt und $\mathfrak{K}$ ist die Gesamtheit aller so entstehenden Zahlen. Wenn nun S eine beliebige der N Substitutionen ist, welche der Körper $\mathfrak{K}$ zuläßt, so resultiert aus ihr offenbar auch für jeden der in $\mathfrak{K}$ enthaltenen Körper $\mathfrak{k}$, $\mathfrak{k}^{(1)}$, $\mathfrak{k}^{(2)}, \cdots, \mathfrak{k}^{(n-1)}$ eine ganz bestimmte Substitution, bei welcher aber jede der in $\mathfrak{K}$ enthaltenen Zahlen α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots$, $\alpha^{(n-1)}$ nur in eine Wurzel der Gleichung (97) verwandelt, bei welcher also, weil verschiedene Zahlen des Körpers $\mathfrak{K}$ durch die Substitution S auch in verschiedene Zahlen übergehen, diese Zahlen α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots, \alpha^{(n-1)}$ nur untereinander vertauscht werden können. Somit verwandelt sich jede in $\mathfrak{K}$ enthaltene Zahl ζ als rationale Funktion jener Zahlen mit zu $\mathfrak{R}$ gehörigen, also unverändert bleibenden Koeffizienten in eben dieselbe Funktion jener nur anders geordneten Zahlen, bleibt mithin eine rationale Funktion von α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots, \alpha^{(n-1)}$, d. i. eine Zahl des Körpers $\mathfrak{K}$. Hieraus folgt offenbar zunächst, daß der Körper $\mathfrak{K}$ bei jeder Substitution derselbe, nämlich aus der Gesamtheit derselben Zahlen zusammengesetzt bleibt, d. h. also ein Galoisscher Körper ist.

Wenn ferner die Zahl ζ eine symmetrische Funktion der Zahlen α, $\alpha^{(1)}$, $\alpha^{(2)}, \cdots, \alpha^{(n-1)}$, d. i. der Wurzeln der Gleichung (97) ist, so bleibt sie bei jeder der N Substitutionen des Körpers ungeändert, ist also eine einwertige Zahl desselben Bezeichnet man aber mit ζ, $\zeta^{(1)}$, $\zeta^{(2)}, \cdots, \zeta^{(N-1)}$ die bezüglich irgend eines Körpers N^{ten} Grades konjugierten Werte von ζ, so ergibt sich für die Spur einer einwertigen Zahl ζ die Gleichheit:

$$S(\zeta) = \zeta + \zeta^{(1)} + \zeta^{(2)} + \cdots + \zeta^{(N-1)} = N \cdot \zeta,$$

mithin $\zeta = \frac{S(\zeta)}{N}$, und folglich ist jede einwertige Zahl eines Körpers gleich einer in seinem Rationalitäts-

bereiche enthaltenen Zahl. Man schließt hier also weiter, daß jede symmetrische rationale Funktion der bezüglich des Körpers $\mathfrak{k}$ konjugierten Zahlen α, $\alpha^{(1)}$, $\alpha^{(2)}$, $\cdots$, $\alpha^{(n-1)}$ eine Zahl seines Rationalitätsbereiches ist.

Nun sind diese Zahlen die Wurzeln einer beliebig gegebenen (in $\mathfrak{R}$ irreduktibeln) Gleichung (97). Nimmt man diese Gleichung als die allgemeine Gleichung n^{ten} Grades, d. h. ihre Koeffizienten als Unbestimmte an, so ist sie notwendig irreduktibel und die Koeffizienten sind selbst die Elemente $\mathfrak{R}'$, $\mathfrak{R}''$, $\cdots$ des Rationalitätsbereiches der Gleichung. Hiermit erhält man dann den bekannten Satz aus der Theorie der algebraischen Gleichungen:

Jede symmetrische rationale ganzzahlige Funktion von den *Wurzeln* einer Gleichung ist eine rationale und ganzzahlige Funktion ihrer *Koeffizienten*.[1])

Zweites Kapitel.

Die Moduln.

1. Sondert man aus der Gesamtheit aller in $\mathfrak{R}$ algebraischen Zahlen die ganzen unter ihnen aus, so erhält man ein System von Zahlen, welches sich nach Kap. 1 Nr. 2 durch Addition, Subtraktion und Multiplikation seiner Zahlen reproduziert. Bevor wir nun dazu übergehen, die arithmetischen Eigenschaften dieses Systems der ganzen in $\mathfrak{R}$ algebraischen Zahlen zu untersuchen, ist es von wesentlichem Nutzen, zuvörderst solche Systeme von Zahlen zu betrachten, die wenig-

1) Jede symmetrische *ganze* und ganzzahlige Funktion der *Wurzeln* wird demnach eine *ganze* und ganzzahlige Funktion der *Koeffizienten* sein. Denn, ist $\mathfrak{R}$ der aus den unbestimmten Koeffizienten der allgemeinen Gleichung entspringende Rationalitätsbereich, so ist jede Wurzel dieser Gleichung und somit auch jede ganze und ganzzahlige Funktion ihrer Wurzeln eine in $\mathfrak{R}$ algebraische ganze Größe, jede symmetrische Funktion dieser Art aber zudem auch in $\mathfrak{R}$ enthalten, woraus die Behauptung mittels Kap. 4 Nr. 2 hervorgeht.

stens bei Anwendung der beiden erstgenannten Operationen reproduziert werden.

Man nennt jede solche Gesamtheit von Zahlen, welche also durch den Umstand charakterisiert ist, daß die Summe $\alpha' + \alpha''$ und die Differenz $\alpha' - \alpha''$ zweier ihrer Zahlen α', α'' stets wieder eine ihrer Zahlen ist, nach dem Vorgange von Dedekind, der ihre Theorie in weiterem Umfange entwickelt hat,[1]) einen Modulus von Zahlen. Wir müssen uns hier damit begnügen, die einfachsten Sätze, die für Moduln gelten, sofern sie weiterhin notwendig sein werden, abzuleiten.

Der einfachste, doch nur uneigentliche Modulus ist offenbar die einzelne Zahl Null; sie ist in jedem anderen Modulus enthalten, da ein solcher mit der Zahl α zugleich auch die Differenz $\alpha - \alpha = 0$ enthält. Wenn wir aber in der Folge von diesem Modulus absehen, so wäre der elementarste von allen die Gesamtheit der (positiven und negativen) rationalen ganzen Zahlen; er soll im folgenden stets durch das Zeichen $\mathfrak{z}$ ausgedrückt werden. Desgleichen bilden ersichtlich sämtliche Vielfachen einer rationalen ganzen Zahl m einen in $\mathfrak{z}$ enthaltenen Modulus $\mathfrak{m}$; und, wenn d ein Teiler von m ist, so machen allgemeiner die Vielfachen von d wieder einen Modulus $\mathfrak{d}$ aus, in welchem der ebengenannte gleichfalls enthalten ist.

Der Umstand, daß ein Modulus $\mathfrak{m}$ in einem andern Modulus $\mathfrak{m}'$ enthalten ist, d. h. daß alle seine Zahlen zugleich auch Zahlen des letztern Modulus sind, soll durch das Zeichen

$$\mathfrak{m} \succ \mathfrak{m}' \tag{1}$$

ausgedrückt werden. Wenn aber der so bezeichnete Umstand stattfindet, soll $\mathfrak{m}$ teilbar heißen durch $\mathfrak{m}'$, oder $\mathfrak{m}'$ ein Teiler von $\mathfrak{m}$ genannt werden.

Diese scheinbar den Sachverhalt verkehrende Ausdrucks-

---

1) Dedekind, sur la théorie des nombres entiers algébriques, Paris, Gauthier-Villars, 1877, extrait du Bulletin des sc. mathém. et astron. (1) 9 et (2) 1; ferner Dirichlets Vorlesungen über Zahlentheorie, herausgeg. von Dedekind, 4. Aufl., 1894, p. 493.

weise wird gleichwohl durch die Folge, wie schon durch das voraufgehende Beispiel gerechtfertigt; denn in diesem durch die Formel $\mathfrak{m} \succ \mathfrak{d}$ bezeichneten Falle entspricht in der Tat der Modulus $\mathfrak{d}$, obwohl er umfassender ist als der Modulus $\mathfrak{m}$, einem Teiler d von der Zahl m, welcher der Modulus $\mathfrak{m}$ entspricht, und darf daher passend ebenfalls ein Teiler von $\mathfrak{m}$ genannt werden.

Enthält ein Modulus $\mathfrak{m}$ die Eins, so enthält er auch jede rationale ganze Zahl, d. h. den gesamten Modulus $\mathfrak{z}$, wie denn auch das Umgekehrte von selbst einleuchtet; jener Umstand ist also identisch mit der Bedingung $\mathfrak{z} \succ \mathfrak{m}$.

Da, wenn gleichzeitig

$$\mathfrak{m} \succ \mathfrak{n}, \quad \mathfrak{n} \succ \mathfrak{m} \tag{2}$$

ist, die Zahlen eines jeden der beiden Moduln $\mathfrak{m}, \mathfrak{n}$ auch Zahlen des andern sind, so bilden diese beiden die gleiche Gesamtheit von Zahlen, was durch die Gleichheit

$$\mathfrak{m} = \mathfrak{n} \tag{3}$$

ausgedrückt werden soll; die beiden Bedingungen (2) sind also mit dieser Gleichheit identisch: zwei Moduln, deren jeder ein Teiler des andern ist, sind einander gleich.

Sind $\mathfrak{a}, \mathfrak{b}$ zwei Zahlenmoduln und bedeutet α jede Zahl des ersten, β jede Zahl des zweiten, so bildet die Gesamtheit aller Zahlen $\alpha + \beta$ wieder einen Modulus, der durch das Zeichen $\mathfrak{a} + \mathfrak{b}$ oder $\mathfrak{b} + \mathfrak{a}$ angezeigt werden soll; denn, sind α', α'' irgend zwei Zahlen in $\mathfrak{a}$, und β', β'' irgend zwei solche in $\mathfrak{b}$, so gehören, da dann auch

$$\alpha' \pm \alpha'', \quad \beta' \pm \beta''$$

bezw. in $\mathfrak{a}$ und $\mathfrak{b}$ enthalten sind, mit $\alpha' + \beta'$, $\alpha'' + \beta''$ zugleich auch die Zahlen

$$(\alpha' + \beta') \pm (\alpha'' + \beta'') = (\alpha' \pm \alpha'') + (\beta' \pm \beta'')$$

der Gesamtheit $\alpha + \beta$ an.

Da zu den Zahlen α wie β auch die Null gehört, so enthält der Modulus $\mathfrak{a} + \mathfrak{b}$ sowohl sämtliche Zahlen α des Modulus $\mathfrak{a}$, als auch sämtliche Zahlen β des Modulus $\mathfrak{b}$, so daß man setzen darf

$$\mathfrak{a} \succ \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{b} \succ \mathfrak{a} + \mathfrak{b};$$

mithin ist der Modulus $\mathfrak{a} + \mathfrak{b}$ gemeinsamer Teiler von $\mathfrak{a}$ und $\mathfrak{b}$. Ist aber $\mathfrak{m}$ irgend ein gemeinsamer Teiler dieser Moduln:

$$\mathfrak{a} \succ \mathfrak{m}, \quad \mathfrak{b} \succ \mathfrak{m},$$

so sind mit allen Zahlen α von $\mathfrak{a}$ und allen Zahlen β von $\mathfrak{b}$ zugleich auch alle Zahlen $\alpha + \beta$ von $\mathfrak{a} + \mathfrak{b}$ in $\mathfrak{m}$ enthalten, mithin $\mathfrak{m}$ ein Teiler von $\mathfrak{a} + \mathfrak{b}$. Da endlich auch umgekehrt jeder solcher Teiler mit $\mathfrak{a} + \mathfrak{b}$ zugleich auch $\mathfrak{a}$ und $\mathfrak{b}$ in sich enthält, also gemeinsamer Teiler dieser beiden Moduln ist, ergibt sich der Satz: die gemeinsamen Teiler zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ stimmen überein mit den sämtlichen Teilern des Modulus $\mathfrak{a} + \mathfrak{b}$, der selbst ein gemeinsamer Teiler ist und deshalb, obwohl an Umfang am kleinsten, in Analogie mit der Theorie der rationalen ganzen Zahlen, der *größte* gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}$ genannt werden soll.

Ist der größte gemeinsame Teiler zweier Moduln gleich einem von ihnen, so ist dieser ein Teiler des andern und umgekehrt. Denn aus $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$ folgt wegen $\mathfrak{a} \succ \mathfrak{a} + \mathfrak{b}$ die Beziehung $\mathfrak{a} \succ \mathfrak{b}$; umgekehrt, so oft $\mathfrak{a} \succ \mathfrak{b}$ ist, sind mit den Zahlen α von $\mathfrak{a}$ auch alle Zahlen $\alpha + \beta$ in $\mathfrak{b}$ enthalten, also ist $\mathfrak{a} + \mathfrak{b} \succ \mathfrak{b}$, da aber auch umgekehrt $\mathfrak{b} \succ \mathfrak{a} + \mathfrak{b}$ ist, so ergibt sich die Gleichheit von $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{b}$.

Endlich leuchtet unmittelbar aus dem Sinne des Zeichens $\succ$ ein, daß, so oft

$$\mathfrak{a} \succ \mathfrak{a}', \quad \mathfrak{b} \succ \mathfrak{b}'$$

ist, auch

$$\mathfrak{a} + \mathfrak{b} \succ \mathfrak{a}' + \mathfrak{b}'$$

sein muß.

Zu einem ferneren Grundbegriffe gelangt man, wenn man die Gesamtheit aller Zahlen ins Auge faßt, welche zugleich in zwei gegebenen Moduln $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind; auch diese Gesamtheit ist wieder ein Modulus, welcher nach *Dedekinds* Vorgange mit $\mathfrak{a} - \mathfrak{b}$ oder $\mathfrak{b} - \mathfrak{a}$ bezeichnet werde. Sind nämlich γ', γ'' irgend zwei derselben angehörige, also beide sowohl in $\mathfrak{a}$ als in $\mathfrak{b}$ vorhandene Zahlen, so gehören der Definition eines Modulus zufolge auch die Zahlen $\gamma' \pm \gamma''$ sowohl zu $\mathfrak{a}$ wie zu $\mathfrak{b}$ und demnach auch zu der gedachten

Gesamtheit, charakterisieren diese somit als Modulus. Da nun gleichzeitig

$$\mathfrak{a} - \mathfrak{b} \succ \mathfrak{a}, \quad \mathfrak{a} - \mathfrak{b} \succ \mathfrak{b},$$

d. i. $\mathfrak{a} - \mathfrak{b}$ sowohl durch $\mathfrak{a}$ wie durch $\mathfrak{b}$ teilbar ist, darf der Modulus $\mathfrak{a} - \mathfrak{b}$ ein gemeinsames Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ genannt werden. Ist aber $\mathfrak{m}$ irgend ein gemeinsames Vielfache derselben, so daß $\mathfrak{m}$ sowohl in $\mathfrak{a}$ wie in $\mathfrak{b}$ enthalten ist, so muß $\mathfrak{m}$ offenbar auch in $\mathfrak{a} - \mathfrak{b}$ enthalten, durch $\mathfrak{a} - \mathfrak{b}$ teilbar oder ein Vielfaches von $\mathfrak{a} - \mathfrak{b}$ sein; und umgekehrt wird jedes Vielfache $\mathfrak{m}$ von $\mathfrak{a} - \mathfrak{b}$ wegen $\mathfrak{m} \succ \mathfrak{a} - \mathfrak{b}$ auch die Bedingungen $\mathfrak{m} \succ \mathfrak{a}$, $\mathfrak{m} \succ \mathfrak{b}$ gleichzeitig erfüllen, d. i. ein gemeinsames Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ sein. Somit ergibt sich der Satz: Die gemeinsamen Vielfachen zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ stimmen überein mit den sämtlichen Vielfachen des Modulus $\mathfrak{a} - \mathfrak{b}$, welcher selbst ein gemeinsames Vielfache ist und deshalb, obwohl an Umfang am größten, das *kleinste* gemeinsame Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ genannt werden soll.

Ist das kleinste gemeinsame Vielfache zweier Moduln gleich einem von ihnen, so ist dieser teilbar durch den andern, und umgekehrt. Denn, ist $\mathfrak{a} - \mathfrak{b} = \mathfrak{b}$, so sind eben alle Zahlen von $\mathfrak{b}$ auch solche von $\mathfrak{a}$, d. i. $\mathfrak{b} \succ \mathfrak{a}$; umgekehrt aber folgt aus dieser Beziehung, daß die Zahlen, welche $\mathfrak{b}$ mit $\mathfrak{a}$ gemeinsam hat, mit den sämtlichen Zahlen von $\mathfrak{b}$ identisch sind.

Endlich folgt wieder aus

$$\mathfrak{a} \succ \mathfrak{a}', \quad \mathfrak{b} \succ \mathfrak{b}'$$

auch

$$\mathfrak{a} - \mathfrak{b} \succ \mathfrak{a}' - \mathfrak{b}',$$

denn die $\mathfrak{a}$ und $\mathfrak{b}$ gemeinsamen Zahlen werden, weil einerseits in $\mathfrak{a}'$, und andererseits in $\mathfrak{b}'$ enthalten, auch $\mathfrak{a}'$ und $\mathfrak{b}'$ gemeinsam, d. i. in $\mathfrak{a}' - \mathfrak{b}'$ enthalten sein.

Unter den mannigfachen Folgerungen, die aus diesen Definitionen zu ziehen sind, heben wir nur den einen Satz hervor, der sich in nachstehender, für irgend drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gültigen Formel ausspricht:

$$\mathfrak{a} - (\mathfrak{b} - \mathfrak{c}) = (\mathfrak{a} - \mathfrak{b}) - \mathfrak{c}; \tag{4}$$

in der Tat bezeichnet die eine, wie die andere Seite dieser Gleichheit nur auf verschiedene Weise die Gesamtheit der Zahlen, welche allen drei Moduln gemeinsam sind.

2. Bedeutet wieder α jede Zahl in $\mathfrak{a}$, β jede Zahl in $\mathfrak{b}$, so ist offenbar die Gesamtheit der Produkte $\alpha\beta$ und der aus solchen durch Addition oder Subtraktion entstehenden Zahlen ein neuer Modulus, welcher das Produkt der Moduln $\mathfrak{a}, \mathfrak{b}$ genannt und mit $\mathfrak{ab}$ oder $\mathfrak{ba}$ bezeichnet werden soll. Diese Definition dehnt sich sogleich auf das Produkt einer beliebigen Anzahl von Faktoren aus, und man erkennt auch unmittelbar aus ihr, daß die Faktoren des Produkts beliebig vertauscht werden dürfen, nicht minder, daß die Multiplikation von Moduln assoziativ ist, d. h. daß die Gleichheit besteht:

$$(5)\qquad (\mathfrak{ab})\cdot\mathfrak{c} = \mathfrak{a}\cdot(\mathfrak{bc}).$$

Aus der Bedeutung des Produkts mehrerer Moduln ergibt sich sogleich die Bedeutung der Potenz $\mathfrak{a}^n$ eines Modulus $\mathfrak{a}$ als des Produkts aus n gleichen Faktoren $\mathfrak{a}$.

Für jeden Modulus $\mathfrak{a}$ ist ferner

$$(6)\qquad \mathfrak{a}\mathfrak{z} = \mathfrak{a}.$$

Denn, ist z irgend eine rationale ganze, d. i. zu $\mathfrak{z}$ gehörige Zahl, so gehört der Definition eines Modulus zufolge das Produkt $z\alpha$ und folglich auch jede Summe oder Differenz solcher Produkte dem Modulus $\mathfrak{a}$ an, der umgekehrt, da jede seiner Zahlen α gleich $\alpha\cdot 1$ gesetzt werden kann, in $\mathfrak{a}\mathfrak{z}$ enthalten ist. Die Gleichung (6) ist zudem für den Modulus $\mathfrak{z}$ charakteristisch, insofern er der einzige ist, der sie für jeden Modulus $\mathfrak{a}$ erfüllt; denn, wäre stets $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$, so müßte auch $\mathfrak{z}\mathfrak{m} = \mathfrak{z}$, d. h. aber $\mathfrak{m} = \mathfrak{z}$ sein.

Aus $\mathfrak{a} \succ \mathfrak{a}'$, $\mathfrak{b} \succ \mathfrak{b}'$ folgt wieder $\mathfrak{ab} \succ \mathfrak{a}'\mathfrak{b}'$; denn nach den Voraussetzungen ist jedes Produkt $\alpha\beta$ auch das Produkt einer Zahl aus $\mathfrak{a}'$ in eine Zahl aus $\mathfrak{b}'$ und folglich auch jedes Aggregat solcher Produkte im Modulus $\mathfrak{a}'\mathfrak{b}'$ enthalten.

Insbesondere besteht also, da immer $\mathfrak{a} \succ \mathfrak{a}$ ist, wegen $\mathfrak{z}\mathfrak{a} = \mathfrak{a}$ die Beziehung

$$(7)\qquad \mathfrak{a} \succ \mathfrak{ab}, \quad \text{so oft} \quad \mathfrak{z} \succ \mathfrak{b}$$

ist.

Aus der Fülle von Sätzen, die aus diesen Definitionen gefolgert werden können, entnehmen wir nur den einen besonders wichtigen, für irgend drei Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ geltenden, der sich ausspricht in der Formel:

$$(\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}. \tag{8}$$

In der Tat, ist α jede Zahl in $\mathfrak{a}$, β jede Zahl in $\mathfrak{b}$, γ jede Zahl in $\mathfrak{c}$, so ist jedes Produkt $(\alpha + \beta) \cdot \gamma$ aus einer Zahl in $\mathfrak{a} + \mathfrak{b}$ und einer Zahl in $\mathfrak{c}$ die Summe $\alpha\gamma + \beta\gamma$ aus einer zu $\mathfrak{a}\mathfrak{c}$ und einer zu $\mathfrak{b}\mathfrak{c}$ gehörigen Zahl und ist also, ebenso wie auch jedes Aggregat mehrerer solcher Produkte in $\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ enthalten; also ist erstens

$$(\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c} \succ \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}.$$

Da andererseits

$$\mathfrak{a} \succ \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{b} \succ \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{c} \succ \mathfrak{c}$$

ist, ergibt sich

$$\mathfrak{a}\mathfrak{c} \succ (\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c}, \quad \mathfrak{b}\mathfrak{c} \succ (\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c},$$

woraus der Definition eines Modulus zufolge offenbar zweitens

$$\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c} \succ (\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c}$$

folgt. Beides zusammen bestätigt die Gleichung (8).

In Anwendung hiervon ergibt sich dann weiter die allgemeine Beziehung:

$$(\mathfrak{a} + \mathfrak{b} + \mathfrak{c})(\mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b}) = (\mathfrak{b} + \mathfrak{c}) \cdot (\mathfrak{c} + \mathfrak{a}) \cdot (\mathfrak{a} + \mathfrak{b}), \tag{9}$$

von der wir später einen sehr bedeutsamen Gebrauch zu machen gedenken. Denn, werden die beiden Ausdrücke nach den voraufgehenden Regeln, nämlich ganz nach den gewöhnlichen Regeln der algebraischen Multiplikation entwickelt, so erhält man links die Summe:

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} + \mathfrak{a}^2\mathfrak{b} + \mathfrak{a}^2\mathfrak{c} + \mathfrak{b}^2\mathfrak{c} + \mathfrak{a}\mathfrak{b}\mathfrak{c} + \mathfrak{b}^2\mathfrak{a} + \mathfrak{c}^2\mathfrak{a} + \mathfrak{c}^2\mathfrak{b} + \mathfrak{a}\mathfrak{b}\mathfrak{c},$$

rechts aber diese Summe:

$$\mathfrak{a}\mathfrak{b}\mathfrak{c} + \mathfrak{a}^2\mathfrak{b} + \mathfrak{a}\mathfrak{c}^2 + \mathfrak{a}^2\mathfrak{c} + \mathfrak{b}^2\mathfrak{c} + \mathfrak{b}^2\mathfrak{a} + \mathfrak{b}\mathfrak{c}^2 + \mathfrak{a}\mathfrak{b}\mathfrak{c},$$

die mit der ersteren gleichbedeutend ist, da offenbar die Summe zweier gleichen Moduln $\mathfrak{m}$ mit $\mathfrak{m}$ identisch ist:

$$\mathfrak{m} + \mathfrak{m} = \mathfrak{m}. \tag{10}$$

Ist α jede Zahl eines Modulus $\mathfrak{a}$ und β eine gegebene, von Null verschiedene Zahl, so bilden er-

sichtlich alle Zahlen $\alpha\beta$ einen Modulus, welcher $\mathfrak{a}\beta$ heiße. Ist $\mathfrak{a}'$ ein zweiter Modulus und $\mathfrak{a}\beta \succ \mathfrak{a}'\beta$, so ist offenbar jede Zahl $\alpha\beta$ gleich einer in $\mathfrak{a}'\beta$ enthaltenen, d. i. α eine in $\mathfrak{a}'$ enthaltene Zahl, mithin folgt $\mathfrak{a} \succ \mathfrak{a}'$. Aus $\mathfrak{a}\beta = \mathfrak{a}'\beta$ ergibt sich daher $\mathfrak{a} = \mathfrak{a}'$.

Sei nun $\mathfrak{m}$ ein anderer Modulus, so bildet die Gesamtheit aller Zahlen β, für welche $\mathfrak{a}\beta \succ \mathfrak{m}$ ist, wie leicht zu ersehen, wieder einen Modulus, welcher $\mathfrak{b}$ heiße. Denn, sind β', β'' irgend zwei solche Zahlen, so gehören, wenn wieder α jede Zahl in $\mathfrak{a}$ bedeutet, die Produkte $\alpha\beta', \alpha\beta''$ der Annahme nach und folglich auch die Produkte $\alpha(\beta' \pm \beta'')$ dem Modulus $\mathfrak{m}$, d. h. die Zahlen $\beta' \pm \beta''$ der gedachten Gesamtheit an, die mithin ein Modulus $\mathfrak{b}$ ist von der Beschaffenheit, daß

$$\mathfrak{a}\mathfrak{b} \succ \mathfrak{m}. \tag{11}$$

Der so definierte Modulus $\mathfrak{b}$ wird von *Dedekind* als *Quotient* der Moduln $\mathfrak{a}, \mathfrak{m}$ mit

$$\mathfrak{b} = \frac{\mathfrak{m}}{\mathfrak{a}} \tag{12}$$

bezeichnet.

Er genießt einer ausgezeichneten Eigenschaft in dem Falle, daß $\mathfrak{a}$ und $\mathfrak{m}$ ein- und denselben Modulus bedeuten, in welchem Falle wir den Modulus $\mathfrak{b}$ mit $\mathfrak{a}^0$ anzeigen wollen, so daß

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}} \tag{13}$$

ist. Sind nämlich $\alpha_1{}^0, \alpha_2{}^0$ irgend zwei Zahlen in $\mathfrak{a}^0$, so ist der Definition zufolge

$$\mathfrak{a}\alpha_1{}^0 \succ \mathfrak{a},$$

d. h., wenn α irgend eine Zahl in $\mathfrak{a}$ bedeutet, so ist $\alpha\alpha_1{}^0$ gleich einer in $\mathfrak{a}$ enthaltenen Zahl α', demnach ist, da auch $\mathfrak{a}\alpha_2{}^0 \succ \mathfrak{a}$ sein soll, $\alpha'\alpha_2{}^0$ oder $\alpha \cdot \alpha_1{}^0\alpha_2{}^0$ wieder in $\mathfrak{a}$ enthalten, mit andern Worten: $\alpha_1{}^0\alpha_2{}^0$ ist wieder eine in $\mathfrak{a}^0$ enthaltene Zahl. Somit reproduzieren sich die Zahlen des besonderen Modulus $\mathfrak{a}^0$ nicht nur durch Addition und Subtraktion, sondern auch durch Multiplikation, derart, daß jedenfalls

$$\mathfrak{a}^0 \cdot \mathfrak{a}^0 \succ \mathfrak{a}^0 \tag{14}$$

ist. Zu den Zahlen des Modulus $\mathfrak{a}^0$ gehört aber sicher auch

die Eins, da $\alpha \cdot 1$ zugleich mit α in $\mathfrak{a}$ enthalten ist; demnach ist $\mathfrak{z} \succ \mathfrak{a}^0$, daher auch $\mathfrak{z}\mathfrak{a}^0$ oder $\mathfrak{a}^0 \succ \mathfrak{a}^0 \cdot \mathfrak{a}^0$. Mit der soeben gewonnenen Beziehung zusammen ergibt sich hieraus die Gleichheit

$$\mathfrak{a}^0 \cdot \mathfrak{a}^0 = \mathfrak{a}^0. \tag{15}$$

Hier führen wir einen neuen für die Folge außerordentlich wichtigen Begriff ein, den *einer Ordnung* $\mathfrak{o}$ *von Zahlen*. Wir nennen so jeden Zahlenmodulus, der die Eins in sich enthält und sich durch Multiplikation reproduziert, oder welcher die beiden Bedingungen erfüllt:

$$\mathfrak{z} \succ \mathfrak{o}, \quad \mathfrak{o} \cdot \mathfrak{o} \succ \mathfrak{o}, \tag{16}$$

deren zweite dem eben Gesagten entsprechend schärfer als die Gleichheit

$$\mathfrak{o} \cdot \mathfrak{o} = \mathfrak{o} \tag{16a}$$

gefaßt werden kann.

Dieser Definition zufolge ist also der zu irgend einem Modulus $\mathfrak{a}$ gehörige Quotient $\mathfrak{a}^0$ eine Ordnung. Aber auch umgekehrt ist jede Ordnung $\mathfrak{o}$ ein Quotient, nämlich der Quotient $\mathfrak{o}^0 = \frac{\mathfrak{o}}{\mathfrak{o}}$; denn der zweiten Bedingung (16) gemäß ist $\mathfrak{o}$ jedenfalls in diesem Quotienten $\mathfrak{o}^0$ enthalten, aus der ersten jener Bedingungen folgt aber auch umgekehrt

$$\mathfrak{o}^0 = \mathfrak{z}\mathfrak{o}^0 \succ \mathfrak{o}\mathfrak{o}^0 \succ \mathfrak{o},$$

und somit die Gleichheit $\mathfrak{o} = \mathfrak{o}^0$.

3. Ist $\mathfrak{m}$ ein gegebener Modulus, so sollen zwei Zahlen α, β einander kongruent heißen in bezug auf diesen Modulus, in Zeichen:

$$\alpha \equiv \beta \pmod{\mathfrak{m}}, \tag{17}$$

wenn ihre Differenz eine in $\mathfrak{m}$ enthaltene Zahl ist.

Nach dieser Definition sind offenbar die Zahlen μ des Modulus $\mathfrak{m}$ selbst durch die Kongruenz

$$\mu \equiv 0 \pmod{\mathfrak{m}}, \tag{18}$$

der sie und sie allein genügen, charakterisiert. Auch folgt unmittelbar aus jener Definition, daß, wenn die Kongruenz (17) zweier Zahlen α, β (mod. $\mathfrak{m}$) besteht, sie auch für jeden Mo-

dulus $\mathfrak{d}$ erfüllt ist, der ein Teiler von $\mathfrak{m}$ ist; wenn nämlich $\alpha - \beta$ eine Zahl in $\mathfrak{m}$ und $\mathfrak{m} \succ \mathfrak{d}$ ist, so ist $\alpha - \beta$ auch eine Zahl in $\mathfrak{d}$, mithin

$$\alpha \equiv \beta \;(\text{mod. } \mathfrak{d}).$$

Desgleichen folgt aus dem gleichzeitigen Bestehen zweier Kongruenzen

$$\alpha \equiv \beta \;(\text{mod. } \mathfrak{m}), \quad \alpha \equiv \beta \;(\text{mod. } \mathfrak{n})$$

auch die dritte:

$$\alpha \equiv \beta \;(\text{mod. } \mathfrak{m} - \mathfrak{n});$$

denn jenen zufolge ist $\alpha - \beta$ eine zugleich in $\mathfrak{m}$ und in $\mathfrak{n}$ enthaltene Zahl.

Offenbar darf endlich die Kongruenz (17), wenn sie besteht, mit einer beliebigen zur Ordnung $\mathfrak{m}^0$ von $\mathfrak{m}$ gehörigen Zahl μ^0 multipliziert werden; denn, da für eine solche jedes Produkt $\mu\mu^0$, wo μ eine Zahl in $\mathfrak{m}$ ist, zu $\mathfrak{m}$ gehört, so wird, wenn (17) besteht, auch $(\alpha - \beta) \cdot \mu^0$ eine in $\mathfrak{m}$ enthaltene Zahl, d. h.

$$\alpha \cdot \mu^0 \equiv \beta \cdot \mu^0 \;(\text{mod. } \mathfrak{m})$$

sein.

Ist gleichzeitig $\alpha \equiv \beta$ und $\alpha \equiv \gamma$ (mod. $\mathfrak{m}$), so ist auch $\beta \equiv \gamma$ (mod. $\mathfrak{m}$), denn mit den Zahlen $\alpha - \beta$ und $\alpha - \gamma$ gehört auch ihre Differenz $(\alpha - \gamma) - (\alpha - \beta) = \beta - \gamma$ dem Modulus $\mathfrak{m}$ an. Zwei Zahlen also, welche derselben dritten Zahl (mod. $\mathfrak{m}$) kongruent sind, sind es auch untereinander. Dieser Umstand gestattet, alle Zahlen in bezug auf einen gegebenen Modulus in *Klassen* zu verteilen, indem man sämtliche Zahlen, die untereinander kongruent sind, in eine Klasse zusammenfaßt; dann werden irgend zwei Zahlen α, β einander kongruent oder inkongruent sein, je nachdem sie in derselben oder in verschiedenen Klassen sich finden; und greift man aus jeder dieser Klassen nach Belieben eine Zahl heraus, so wird die Gesamtheit dieser Klassenrepräsentanten die charakteristische Eigenschaft haben, daß jede beliebige Zahl einem und nur einem derselben (mod. $\mathfrak{m}$) kongruent ist. In Analogie mit der gewöhnlichen Zahlentheorie nennt man solche Gesamtheit auch ein vollständiges Restsystem oder ein System inkongruenter Zahlen (mod. $\mathfrak{m}$).

Statt sämtlicher Zahlen wollen wir uns so nur die Zahlen eines gegebenen Modulus $\mathfrak{a}$ in Klassen (mod. $\mathfrak{m}$) verteilt denken. Es ist möglich, daß die Menge dieser Zahlenklassen unbegrenzt ist; in den Anwendungen, die wir von der Theorie der Moduln zu machen gedenken, wird sie im Gegenteil stets eine endliche sein und dann soll nach Dedekind ihre Anzahl durch das Zeichen $(\mathfrak{a}, \mathfrak{m})$ ausgedrückt werden; Dedekind behält dies Zeichen auch in dem zuerst erwähnten Falle bei, gibt ihm dann aber den Wert Null, damit die für den andern Fall vorzutragenden Sätze auch für jenen ihre Gültigkeit behalten.

Wir denken uns nun $\mathfrak{m}$ insbesondere als das kleinste gemeinsame Vielfache $\mathfrak{a} - \mathfrak{b}$ zweier gegebenen Moduln $\mathfrak{a}, \mathfrak{b}$. Zwei in $\mathfrak{a}$ enthaltene Zahlen α', α'', welche (mod. $\mathfrak{b}$) kongruent sind, werden es auch sein (mod. $\mathfrak{a} - \mathfrak{b}$), denn, wenn die in $\mathfrak{a}$ enthaltene Differenz $\alpha' - \alpha''$ auch in $\mathfrak{b}$ enthalten ist, so gehört sie eben auch zu $\mathfrak{a} - \mathfrak{b}$. Sind aber α', α'' (mod. $\mathfrak{b}$) inkongruent, so sind sie es auch (mod. $\mathfrak{a} - \mathfrak{b}$), denn, gehörte die Differenz $\alpha' - \alpha''$ dem letzteren Modulus an, so fände sie sich wegen $\mathfrak{a} - \mathfrak{b} \succ \mathfrak{b}$ auch im ersteren. Hieraus ersieht man, daß die Verteilung der Zahlen des Modulus $\mathfrak{a}$ in Klassen ganz die gleiche ist, ob man sie (mod. $\mathfrak{b}$) oder (mod. $\mathfrak{a} - \mathfrak{b}$) ausführt; insbesondere muß also stets auch die Anzahl der Klassen die gleiche, also, sei diese endlich oder unendlich,

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{a} - \mathfrak{b}) \tag{19}$$

sein.

Man darf dieser Gleichheit die folgende hinzufügen:

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{b}). \tag{20}$$

Denn, bezeichnen $\alpha', \alpha'', \alpha''', \cdots$ die sämtlichen, sei's in endlicher oder unendlicher Anzahl vorhandenen (mod. $\mathfrak{b}$) inkongruenten Zahlen des Modulus $\mathfrak{a}$, so bezeichnen sie auch ein vollständiges Restsystem des Modulus $\mathfrak{a} + \mathfrak{b}$ in bezug auf den Modulus $\mathfrak{b}$, da jede Zahl $\alpha + \beta$ des ersteren mit α, also mit einer und nur einer der Zahlen $\alpha', \alpha'', \alpha''', \cdots$, welche auch zu $\mathfrak{a} + \mathfrak{b}$ gehören, nach dem letzteren kongruent befunden wird.

Sind ferner $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ drei Moduln, welche die Bedingung erfüllen, daß $\mathfrak{c} \succ \mathfrak{b} \succ \mathfrak{a}$ ist, so besteht die Gleichheit

$$(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{b}, \mathfrak{c}). \tag{21}$$

Um sich hiervon zu überzeugen, wähle man ein vollständiges Restsystem $\alpha', \alpha'', \alpha''', \cdots$ des Modulus $\mathfrak{a}$ (mod. $\mathfrak{b}$); dann werden, da $\mathfrak{b}$ in $\mathfrak{a}$ enthalten ist, die Zahlen in $\mathfrak{a}$ insgesamt durch die Ausdrücke

$$\alpha' + \beta, \quad \alpha'' + \beta, \quad \alpha''' + \beta, \cdots, \tag{22}$$

repräsentiert, wenn darin β sämtliche Zahlen des Modulus $\mathfrak{b}$ durchläuft. Bilden aber $\beta', \beta'', \beta''', \cdots$ ein vollständiges Restsystem von $\mathfrak{b}$ (mod. $\mathfrak{c}$), so stellen ebenso die Ausdrücke

$$\beta' + \gamma, \quad \beta'' + \gamma, \quad \beta''' + \gamma, \cdots \tag{23}$$

alle Zahlen β von $\mathfrak{b}$ dar, wenn man γ sämtliche Zahlen von $\mathfrak{c}$ durchlaufen läßt. Mithin repräsentieren dann die Ausdrücke

$$\begin{cases} \alpha' + \beta' + \gamma, & \alpha'' + \beta' + \gamma, \quad \alpha''' + \beta' + \gamma, \cdots \\ \alpha' + \beta'' + \gamma, & \alpha'' + \beta'' + \gamma, \quad \alpha''' + \beta'' + \gamma, \cdots \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{cases} \tag{24}$$

die sämtlichen Zahlen des Modulus $\mathfrak{a}$. Je zwei verschiedene der vorstehenden Ausdrücke:

$$\alpha^{(i)} + \beta^{(k)} + \gamma, \quad \alpha^{(i')} + \beta^{(k')} + \gamma$$

sind aber, wie leicht ersichtlich, inkongruent (mod. $\mathfrak{c}$); denn, wären sie, also auch die Ausdrücke

$$\alpha^{(i)} + \beta^{(k)} \text{ und } \alpha^{(i')} + \beta^{(k')} \text{ (mod. } \mathfrak{c})$$

kongruent, so müßten diese, da nach der Voraussetzung $\mathfrak{b}$ ein Teiler von $\mathfrak{c}$ ist, es auch (mod. $\mathfrak{b}$), also $\alpha^{(i)} \equiv \alpha^{(i')}$ (mod. $\mathfrak{b}$), d. i. $\alpha^{(i)} = \alpha^{(i')}$ sein; dann wären jedoch $\beta^{(k)} + \gamma$, $\beta^{(k')} + \gamma$ also auch $\beta^{(k)}, \beta^{(k')}$ (mod. $\mathfrak{c}$) kongruent, d. h. $\beta^{(k)} = \beta^{(k')}$, und die gedachten beiden Ausdrücke nicht verschieden. Hieraus schließt man, daß die Ausdrücke (24) ein vollständiges Restsystem des Modulus $\mathfrak{a}$ (mod. $\mathfrak{c}$) repräsentieren, und damit die Richtigkeit der behaupteten Gleichheit, wenn man noch bedenkt, daß die Menge der Ausdrücke (24) dann und nur dann unendlich ist, wenn wenigstens eine der beiden Mengen (22) und (23) es ist.

Bedeuten wieder $\alpha', \alpha'', \alpha''', \cdots$ ein vollständiges Restsystem (mod. $\mathfrak{b}$) oder, was nach dem Obigen dasselbe ist,

(mod. $\mathfrak{a}-\mathfrak{b}$) für die Zahlen des Modulus $\mathfrak{a}$ und α eine beliebige Zahl in dem letzteren, so bilden auch die Zahlen

$$\alpha+\alpha', \quad \alpha+\alpha'', \quad \alpha+\alpha''', \cdots$$

solch vollständiges Restsystem, und demnach müssen diese Zahlen in ihrer Gesamtheit, d. h. abgesehen von ihrer Reihenfolge, denjenigen des ersteren Systems, und also auch die Summe jener der Summe dieser kongruent sein. Ist demnach $(\mathfrak{a}, \mathfrak{b})$ eine endliche Anzahl, so ergibt sich durch Addition die Kongruenz

$$(\mathfrak{a}, \mathfrak{b}) \cdot \alpha \equiv 0 \ (\text{mod. } \mathfrak{a}-\mathfrak{b}), \tag{25}$$

welche von jeder Zahl α des Modulus $\mathfrak{a}$ erfüllt wird. Offenbar findet sie aber auch in dem Falle statt, wo das vollständige Restsystem aus einer unbegrenzten Menge von Zahlen besteht, weil dann $(\mathfrak{a}, \mathfrak{b}) = 0$ zu denken ist.

Bevor wir diese Betrachtungen über Moduln im allgemeinsten Sinne beschließen, wollen wir eine Aufgabe lösen, die uns später mehrfach entgegentreten wird, nämlich die Aufgabe: alle Zahlen ω zu ermitteln, welche den beiden Kongruenzen

$$\omega \equiv \varrho \ (\text{mod. } \mathfrak{a}), \quad \omega \equiv \sigma \ (\text{mod. } \mathfrak{b}), \tag{26}$$

in denen $\mathfrak{a}, \mathfrak{b}$ gegebene Moduln, ϱ, σ gegebene Zahlen bedeuten, Genüge leisten. Damit es solche Zahlen ω gebe, bedarf es zunächst der Erfüllung einer notwendigen Bedingung, die aber zugleich auch hinreichend ist: es muß

$$\varrho \equiv \sigma \ (\text{mod. } \mathfrak{a}+\mathfrak{b}) \tag{27}$$

sein. In der Tat, da $\omega-\varrho$ in $\mathfrak{a}$, $\omega-\sigma$ in $\mathfrak{b}$ enthalten sein soll, diese Moduln aber beide in $\mathfrak{a}+\mathfrak{b}$ enthalten sind, so müssen jene beiden Zahlen und daher auch ihre Differenz $\varrho-\sigma$ in dem letztern Modulus enthalten sein; ist aber umgekehrt, wenn wir mit α eine Zahl in $\mathfrak{a}$, mit β eine Zahl in $\mathfrak{b}$ bezeichnen,

$$\varrho-\sigma = \alpha+\beta,$$

nämlich gleich einer in $\mathfrak{a}+\mathfrak{b}$ enthaltenen Zahl, so ist die Zahl

$$\omega_0 = \varrho-\alpha = \sigma+\beta$$

gewiß eine Zahl, wie die Kongruenzen (26) sie fordern, nämlich

$$\omega_0 \equiv \varrho \ (\text{mod. } \mathfrak{a}), \quad \omega_0 \equiv \sigma \ (\text{mod. } \mathfrak{b}). \tag{28}$$

Jede andere Zahl ω derselben Art wird mithin mit ω_0 sowohl (mod. $\mathfrak{a}$) als auch (mod. $\mathfrak{b}$) kongruent und daher, früher Bemerktem zufolge, auch

$$(29) \qquad \omega \equiv \omega_0 \text{ (mod. } \mathfrak{a} - \mathfrak{b})$$

sein, wie denn auch umgekehrt jede so bestimmte Zahl ω, da für sie die Differenz $\omega - \omega_0$ sowohl in $\mathfrak{a}$ als in $\mathfrak{b}$ enthalten ist, nach jedem dieser Moduln mit ω_0 und daher wegen (28) mit ϱ (mod. $\mathfrak{a}$), mit σ (mod. $\mathfrak{b}$) kongruent, d. i. eine der gesuchten Zahlen sein wird. Ist demnach die für die Möglichkeit der Kongruenzen (26) erforderliche Bedingung (27) erfüllt, so gibt es unendlich viel Lösungen derselben, welche eine einzige Klasse (mod. $\mathfrak{a} - \mathfrak{b}$) ausmachen, nämlich aus einer unter ihnen, ω_0, durch die Kongruenz (29) bestimmt werden.

4. Nunmehr beschränken wir unsere Untersuchung auf eine besondere Art von Moduln, welche *endliche* Moduln genannt werden mögen. Denkt man sich nämlich aus irgend welchen m Zahlen $\mu_1, \mu_2, \cdots, \mu_m$ die Linearform

$$(30) \qquad f = \mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_m u_m$$

gebildet, so macht die Gesamtheit von unendlich vielen Zahlen, welche man daraus erhält, indem man die Unbestimmten u_i alle rationalen ganzen Zahlen durchlaufen läßt, offenbar einen Zahlenmodulus $\mathfrak{m}$ aus, den wir durch das Symbol

$$(31) \qquad \mathfrak{m} = [\mu_1, \mu_2, \cdots, \mu_m]$$

anzeigen wollen. Derartige Moduln sollen endliche Moduln heißen.

Aus dieser Definition folgt sogleich der Satz: daß das Produkt zweier endlichen Moduln wieder ein endlicher Modulus ist. Wenn nämlich

$$\mathfrak{n} = [\nu_1, \nu_2, \cdots, \nu_n]$$

ein zweiter endlicher Modulus, d. h. die Gesamtheit der Zahlen ist, welche aus der Linearform

$$(32) \qquad \varphi = \nu_1 u_1 + \nu_2 u_2 + \cdots + \nu_n u_n$$

hervorgehen, wenn darin die Unbestimmten u_i alle rationalen ganzen Zahlen durchlaufen, so ist das Produkt $\mathfrak{m} \cdot \mathfrak{n}$ der endliche, durch das Symbol

(33) $[\mu_1\nu_1, \mu_1\nu_2, \cdots, \mu_1\nu_n, \mu_2\nu_1, \cdots, \mu_m\nu_n]$
bezeichnete Modulus oder, wie wir kurz schreiben:

(34) $$\mathfrak{m}\cdot\mathfrak{n} = [\cdots, \mu_i\nu_k, \cdots].$$

In der Tat ist einerseits jedes Produkt aus einer Zahl von der Form (30) und einer von der Form (32) mit ganzzahligen Werten der Unbestimmten und daher auch jede Summe solcher Produkte, d. h. jede Zahl des Modulus $\mathfrak{m}\cdot\mathfrak{n}$ eine homogene lineare Form der Produkte $\mu_i\nu_k$ mit ganzzahligen Koeffizienten, also im Modulus (33) enthalten; andererseits ist jedes der in diesem Modulus enthaltenen Produkte $\mu_i\nu_k$ und daher auch jede linear mittels ganzzahliger Koeffizienten aus ihnen gebildete, d. h. in demselben Modulus enthaltene Zahl eine Zahl des Modulus $\mathfrak{m}\cdot\mathfrak{n}$, und somit die Gleichung (34) erwiesen.

Ebenso überzeugt man sich von der Richtigkeit der Formel

(35) $$\mathfrak{m}+\mathfrak{n} = [\mu_1, \mu_2, \cdots, \mu_m, \nu_1, \nu_2, \cdots, \nu_n],$$

mithin ist der größte gemeinsame Teiler zweier endlichen Moduln wieder ein solcher Modulus.

Daß derselbe Satz auch richtig ist für das kleinste gemeinsame Vielfache zweier endlichen Moduln, erkennt man aus dem folgenden allgemeineren Satze, zu dessen Beweis wir sogleich uns wenden:

Jeder in einem endlichen Modulus $\mathfrak{m}$ enthaltene Modulus ist wieder ein endlicher Modulus.

Nennt man die Zahlen $\mu_1, \mu_2, \cdots, \mu_m$ die Elemente des Modulus (31), so wird man diesen selbst als einen Modulus mit m Elementen bezeichnen können. Der Satz kann dann genauer dahin gefaßt werden, daß die Anzahl der Elemente für den in $\mathfrak{m}$ enthaltenen Modulus die gleiche ist wie für $\mathfrak{m}$. Wir beweisen nun diesen Satz zunächst für jeden Modulus $\mathfrak{m}$ mit einem Elemente, also von der Form

$$\mathfrak{m} = [\mu_1],$$

d. i. für die Gesamtheit aller Vielfachen $\mu_1\cdot u$ von μ_1. Ist nämlich $\mathfrak{a}$ ein in $\mathfrak{m}$ enthaltener Modulus, so haben seine sämtlichen Zahlen die gleiche Form $\mu_1\cdot y$, wo y eine rationale ganze Zahl bedeutet; da aber $\mathfrak{a}$ von Null verschieden gedacht wird und zugleich mit $\mu_1\cdot y$ auch $-\mu_1\cdot y$ zu $\mathfrak{a}$ gehört, so

wird in einer jener Zahlen y den kleinsten positiven Wert haben, welcher h heiße. Der Modulus $\mathfrak{a}$ enthält also die Zahl $h \cdot \mu_1$ und folglich auch jedes Vielfache von $h \cdot \mu_1$. Er enthält aber auch nur solche Vielfache, d. h. in jeder andern Zahl in $\mathfrak{a}$ wird y ein Vielfaches von h sein, denn sonst könnte man $y = hq + r$ setzen, wo $0 < r < h$, und der Modulus $\mathfrak{a}$ enthielte, da sowohl $y \cdot \mu_1$ als auch $h \cdot \mu_1$ ihm angehören, auch die Zahl

$$y \cdot \mu_1 - qh \cdot \mu_1 = r \cdot \mu_1$$

während doch die positive Zahl $r < h$ wäre. Hiernach ist $\mathfrak{a}$ die Gesamtheit der Vielfachen von $h\mu_1$, d. i.

$$\mathfrak{a} = [h\mu_1]$$

also ein endlicher Modulus mit einem Elemente.

Ist so der Satz für Moduln mit einem Elemente bewiesen, so nehmen wir ihn jetzt allgemeiner schon als gültig an für alle Moduln mit $m - 1$ Elementen und zeigen dann, daß er auch für Moduln mit m Elementen, infolge des erstgewonnenen Resultats also allgemein gültig ist. Gesetzt also, der Modulus $\mathfrak{a}$ sei im Modulus (31) enthalten; ist er es auch schon in dem einfacheren Modulus

$$[\mu_1, \mu_2, \cdots, \mu_{m-1}],$$

so wäre er in der Tat der Annahme zufolge ein endlicher Modulus. Zwar ist dann die Anzahl seiner Elemente nur $m - 1$, doch kann man sie auch m nennen, indem als m^{tes} Element die Null hinzugefügt werden darf. Im entgegengesetzten Falle finden sich in $\mathfrak{a}$ Zahlen von der Form

$$\alpha = y_1\mu_1 + y_2\mu_2 + \cdots + y_{m-1}\mu_{m-1} + y_m\mu_m,$$

in denen die letzte der rationalen ganzen Zahlen $y_1, y_2, \cdots, y_m$ nicht Null ist, unter ihnen jedenfalls also auch eine Zahl α_0 dieser Form mit kleinstem positivem Werte dieses Koeffizienten y_m, welcher h heiße, sodaß gesetzt werden kann

$$\alpha_0 = z_1\mu_1 + z_2\mu_2 + \cdots + z_{m-1}\mu_{m-1} + h \cdot \mu_m.$$

In jeder anderen Zahl α des Modulus $\mathfrak{a}$ muß dann aber y_m ein Vielfaches von h sein; denn, wäre wieder $y_m = hq + r$ und r von 0 verschieden, so würde in der mit α und α_0 zugleich in $\mathfrak{a}$ enthaltenen Zahl $\alpha - q \cdot \alpha_0$ der Koeffizient von μ_m gegen die Be-

deutung von h positiv und kleiner als h sein. Da hiernach $y_m = h \cdot q$ sein muß, so wird jede Zahl α des Modulus $\mathfrak{a}$ die Gestalt haben:

$$\alpha = q \cdot \alpha_0 + \beta, \tag{36}$$

wo β eine Zahl des Modulus $[\mu_1, \mu_2, \cdots, \mu_{m-1}]$ mit $m-1$ Elementen bedeutet, q aber jede positive oder negative ganze Zahl oder Null sein darf. Sind hiernach nun

$$\alpha' = q'\alpha_0 + \beta', \; \alpha'' = q''\alpha_0 + \beta''$$

irgend zwei Zahlen des Modulus $\mathfrak{a}$, wo β', β'' dem letztgenannten Modulus angehören, so enthält $\mathfrak{a}$ auch die beiden Zahlen

$$(q' \pm q'')\,\alpha_0 + (\beta' \pm \beta''),$$

d. i. jede Zahl von der Form $q \cdot \alpha_0 + (\beta' \pm \beta'')$, wo auch $\beta' \pm \beta''$ dem Modulus $[\mu_1, \mu_2, \cdots, \mu_{m-1}]$ angehört. Mit anderen Worten: die in der Formel (36) auftretenden Zahlen β bilden einen in $[\mu_1, \mu_2, \cdots, \mu_{m-1}]$ enthaltenen, der gemachten Annahme gemäß also endlichen Modulus mit $m-1$ Elementen. Wird dieser etwa durch $[\alpha_1, \alpha_2, \cdots, \alpha_{m-1}]$ bezeichnet, so lehrt die Formel (36) die Gleichheit

$$\mathfrak{a} = [\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}],$$

derzufolge $\mathfrak{a}$ in der Tat als ein endlicher Modulus mit m Elementen erkannt wird.

Das kleinste gemeinsame Vielfache $\mathfrak{a} - \mathfrak{b}$ zweier Moduln $\mathfrak{a}$, $\mathfrak{b}$ ist in jedem der letztern enthalten; sind diese (oder auch nur einer von ihnen) endliche Moduln, so gilt dem eben Bewiesenen zufolge dies auch von $\mathfrak{a} - \mathfrak{b}$, und somit der Satz:

Das kleinste gemeinsame Vielfache zweier endlichen Moduln ist wieder ein endlicher Modulus.

An diese Sätze schließen wir noch einen andern an, welcher einem bekannten Satze über gewöhnliche Zahlen völlig entspricht[1]):

Ist ein endlicher Modulus $\mathfrak{c}$ teilbar durch jeden der endlichen Moduln $\mathfrak{a}$, $\mathfrak{b}$, so ist das Produkt aus $\mathfrak{c}$ und dem größten gemeinsamen Teiler von $\mathfrak{a}$, $\mathfrak{b}$, nämlich der Modulus $(\mathfrak{a}+\mathfrak{b})\cdot\mathfrak{c}$ teilbar durch das Produkt $\mathfrak{a}\mathfrak{b}$. Bezeichnen nämlich allgemein α_i, β_k,

1) Vgl. Kronecker, Vorlesungen über Zahlentheorie, herausgegeben von Hensel, Bd. 1, p. 164.

γ_k die Elemente der drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, so sind die Elemente von $(\mathfrak{a}+\mathfrak{b})\cdot\mathfrak{c}$ die Produkte $(\alpha_i+\beta_k)\cdot\gamma_k = \alpha_i\gamma_k+\beta_k\gamma_k$. Da nun der Annahme zufolge jedes Element γ_k, weil in $\mathfrak{b}$ enthalten, als homogene lineare, ganzzahlige Funktion der β_k, zugleich aber, weil in $\mathfrak{a}$ enthalten, auch als eine solche Funktion der α_i aufgefaßt werden kann, so ist sowohl der erste als auch der zweite der obigen Summanden eine ebensolche Funktion der Produkte $\alpha_i\beta_k$, welche die Elemente des Modulus $\mathfrak{a}\mathfrak{b}$ bilden, daher sind die Elemente von $(\mathfrak{a}+\mathfrak{b})\cdot\mathfrak{c}$ und allgemeiner sämtliche Zahlen dieses Modulus auch Zahlen des Modulus $\mathfrak{a}\mathfrak{b}$, w. z. b. w.

5. Die Definition eines endlichen Modulus läßt sich wesentlich schärfer fassen, wenn wir die Elemente eines solchen in Bezug auf ihre rationale Unabhängigkeit voneinander prüfen. Es besteht nämlich der Satz:

Die Elemente eines jeden endlichen Modulus lassen sich als voneinander unabhängige Zahlen voraussetzen.

Sei, um ihn zu beweisen,

$$\mathfrak{m} = [\mu_1', \mu_2', \cdots, \mu_m'] \tag{37}$$

irgend ein endlicher Modulus. Sind seine m Elemente nicht sämtlich voneinander unabhängig, so wird man doch, indem man je zwei, dann je drei usw. mit einander verknüpft, eine möglichst große Anzahl unabhängiger Zahlen unter ihnen ausfindig machen können, und die größte so ermittelte Anzahl, welche nach der Annahme kleiner als m ist, heiße n. Nehmen wir so etwa an, solche n unabhängige Elemente seien die ersten n derselben:

$$\mu_1', \mu_2', \cdots, \mu_n'.$$

Sämtliche Elemente des Modulus $\mathfrak{m}$ werden dann darstellbar sein in der Form

$$\mu_i' = a_{i1}\mu_1' + a_{i2}\mu_2' + \cdots + a_{in}\mu_n', \tag{38}$$
$$(i = 1, 2, 3, \cdots, m)$$

in welcher die Koeffizienten a_{ik} rationale Zahlen bedeuten. Bezeichnet man mit ν den Generalnenner dieser in endlicher Anzahl vorhandenen Zahlen, sodaß

$$a_{ik} = \frac{\alpha_{ik}}{\nu}$$

gesetzt werden kann, wo nun α_{ik} eine rationale ganze Zahl ist, und setzt man zugleich $\mu_i' = \nu \cdot \nu_i$ für $i = 1, 2, \cdots, n$, so nehmen die Gleichungen (38) die Gestalt an

$$\mu_i' = \alpha_{i1}\nu_1 + \alpha_{i2}\nu_2 + \cdots + \alpha_{in}\nu_n, \quad (i = 1, 2, \cdots, m)$$

derzufolge die Elemente des Modulus $\mathfrak{m}$ und allgemeiner also dessen sämtliche Zahlen im endlichen Modulus

$$[\nu_1, \nu_2, \cdots, \nu_n]$$

enthalten sind. Nach dem obigen Hauptsatze ist daher $\mathfrak{m}$ ein endlicher Modulus

$$[\mu_1, \mu_2, \cdots, \mu_n]$$

mit n offenbar unabhängigen Elementen, da, wenn zwischen diesen eine rationale Abhängigkeit bestände, auch die n, durch sie in homogener linearer Form ausdrückbaren Zahlen μ_1', μ_2', $\cdots$, μ_n' notwendig voneinander abhängig sein müßten, gegen die Annahme.

Man erkennt hieraus, daß, wie behauptet, jeder endliche Modulus $\mathfrak{m}$ als ein solcher dargestellt werden kann:

$$\mathfrak{m} = [\mu_1, \mu_2, \cdots, \mu_n], \tag{39}$$

dessen Elemente voneinander rational unabhängig sind. Ist dann n die Anzahl dieser seiner Elemente, so soll er *ein n-gliedriger Modulus* heißen, und die Gesamtheit $\mu_1, \mu_2, \cdots, \mu_n$ seiner Elemente seine *Basis*.

Diese Basis eines Modulus kann jedoch auf die verschiedenste Weise gewählt werden. Dies beruht auf folgender Überlegung. Wenn

$$f = \mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n \tag{40}$$

die Linearform ist, aus welcher alle Zahlen des Modulus hervorgehen, indem die Unbestimmten u_i alle rationalen ganzen Zahlen durchlaufen, und man setzt

$$u_i = c_{i1}u_1' + c_{i2}u_2' + \cdots + c_{in}u_n', \quad (i = 1, 2, \cdots, n) \tag{41}$$

wo die Koeffizienten c_{ik} ganzzahlige Werte bedeuten, so verwandelt sich die Gleichung (40) in die folgende:

$$f = \mu_1' u_1' + \mu_2' u_2' + \cdots + \mu_n' u_n', \tag{42}$$

wobei

$$\mu_i' = c_{1i}\mu_1 + c_{2i}\mu_2 + \cdots + c_{ni}\mu_n \quad (i = 1, 2, \cdots, n) \tag{43}$$

gedacht wird. Umgekehrt geht, wenn diese n Gleichungen bestehen, die Formel (42) bei Berücksichtigung der Beziehungen (41) in die Formel (40) über. Nun entspricht jedem ganzzahligen Wertsysteme der Unbestimmten u_i' nach (41) auch ein ganzzahliges Wertsystem der Unbestimmten u_i; bei Voraussetzung der Beziehungen (43) wird also jede Zahl des Modulus $[\mu_1', \mu_2', \cdots, \mu_n']$ auch eine Zahl des Modulus $\mathfrak{m}$, also jener in diesem enthalten sein. Werden aber die Koeffizienten c_{ik} so gewählt, daß gemäß den Gleichungen (41) auch umgekehrt jedem ganzzahligen Wertsysteme der Unbestimmten u_i ein ebensolches Wertsystem der Größen u_i' entspricht, was bekanntlich dann und nur dann geschieht, wenn die Determinante

$$| c_{ik} | \quad (\text{für } i, k = 1, 2, \cdots, n)$$

der Gleichungen (41) gleich ± 1 ist, so wird auch jede Zahl des Modulus $\mathfrak{m}$ eine solche des durch die Gleichungen (43) bestimmten Modulus $[\mu_1', \mu_2', \cdots, \mu_n']$, oder $\mathfrak{m}$ selbst in diesem letztern Modulus enthalten sein. In diesem Falle sind demnach beide Moduln identisch oder

$$[\mu_1, \mu_2, \cdots, \mu_n] = [\mu_1', \mu_2', \cdots, \mu_n'],$$

in diesem und nur in diesem Falle ist also das System der durch die Gleichungen (43) definierten, in $\mathfrak{m}$ enthaltenen Zahlen μ_i' eine neue Basis des Modulus $\mathfrak{m}$.

Hiernach erhält man sämtliche mögliche Basen des Modulus $\mathfrak{m}$ aus einer derselben, wenn man in den Gleichungen (43) die ganzzahligen Koeffizienten auf alle mögliche Weise so wählt, daß ihre Determinante gleich ± 1 wird.

6. Dies führt dazu, allgemeiner zu untersuchen, in welcher Beziehung zwei Moduln

$$\mathfrak{m} = [\mu_1, \mu_2, \cdots, \mu_n], \quad \mathfrak{m}' = [\mu_1', \mu_2', \cdots, \mu_n']$$

zu einander stehen, wenn ihre Elemente durch Gleichungen von der Form der Gleichungen (43) mit einander verbunden, die Koeffizienten der letzteren aber beliebige rationale Zahlen sind. Jedoch beschränken wir unsere Untersuchung auf die Voraussetzung, daß die aus den Koeffizienten gebildete Determinante $C = | c_{ik} |$ von Null verschieden sei. Unter dieser Voraussetzung werden die Elemente μ_i stets zugleich mit den Elementen μ_i' rational voneinander unabhängige Zahlen, die beiden Moduln $\mathfrak{m}$ und $\mathfrak{m}'$ also zugleich n-gliedrig sein; wie denn auch umgekehrt, wenn beide Moduln als n-gliedrig vorausgesetzt werden, C von Null verschieden sein muß (s. Kap. 1, Nr. 7).

Dies vorausgeschickt, richten wir unsere Aufmerksamkeit auf den Modulus $\mathfrak{m} - \mathfrak{m}'$, welcher aus den, den beiden Moduln $\mathfrak{m}, \mathfrak{m}'$ gemeinsamen Zahlen besteht. Nennt man ν den Generalnenner aller Koeffizienten c_{ik} in den Gleichungen (43), sodaß man

$$c_{ik} = \frac{\gamma_{ik}}{\nu} \tag{44}$$

setzen kann, wo dann die sämtlichen γ_{ik} ganze rationale Zahlen bezeichnen, so ergibt sich aus jenen Gleichungen

$$\nu \cdot \mu_i' = \gamma_{1i} \cdot \mu_1 + \gamma_{2i} \cdot \mu_2 + \cdots + \gamma_{ni} \cdot \mu_n; \quad (i = 1, 2, \cdots, n) \tag{45}$$

jede der Zahlen $\nu\mu_1', \nu\mu_2', \cdots, \nu\mu_n'$ gehört also sowohl zum Modulus $\mathfrak{m}'$ als zum Modulus $\mathfrak{m}$ und ist mithin auch eine Zahl des Modulus $\mathfrak{m} - \mathfrak{m}'$. Scheidet man also aus dem Modulus $\mathfrak{m}'$ diejenigen Zahlen

$$\lambda = y_1\mu_1' + y_2\mu_2' + \cdots + y_n\mu_n' \tag{46}$$

aus, welche auch zu $\mathfrak{m}$ gehören, oder die Zahlen des Modulus $\mathfrak{m} - \mathfrak{m}'$ sind, so finden sich unter ihnen auch solche, in denen der letzte Koeffizient y_n von Null verschieden ist, z. B. die Zahl $\nu\mu_n'$, und folglich unter den letzteren wieder eine Zahl

$$\lambda = y_1^{(n)}\mu_1' + y_2^{(n)}\mu_2' + \cdots + y_n^{(n)}\mu_n', \tag{47}$$

in welcher dieser Koeffizient den kleinsten positiven Wert $y_n^{(n)}$ hat. Man sieht dann wieder leicht ein, daß in jeder der anderen Zahlen λ der Koeffizient y_n ein Vielfaches von $y_n^{(n)}$ etwa $y_n = z_n y_n^{(n)}$ sein müsse, derart, daß man setzen darf

$$\lambda = \lambda' + z_n \lambda_n, \tag{48}$$

wo λ' eine Zahl des Modulus $[\mu_1', \mu_2', \cdots, \mu_{n-1}']$ ist, welche zugleich mit λ, λ_n in $\mathfrak{m} - \mathfrak{m}'$ enthalten ist. Auch leuchtet ein, daß für jede Zahl λ' dieser Art die durch die Formel (48) bestimmte Zahl λ eine Zahl des Modulus $\mathfrak{m} - \mathfrak{m}'$ sein wird, und daß also diese Formel sämtliche Zahlen des letztern darstellt, wenn z_n alle ganzen rationalen Zahlen, λ' aber die sowohl in $[\mu_1', \mu_2', \cdots, \mu_{n-1}']$, d. i. in der Formel

$$\lambda' = y_1 \mu_1' + y_2 \mu_2' + \cdots + y_{n-1} \mu_{n-1}' \tag{49}$$

als auch in $\mathfrak{m} - \mathfrak{m}'$ enthaltenen Zahlen durchläuft. Da unter den letzteren aber wieder solche Zahlen befindlich sind, in denen der letzte Koeffizient y_{n-1} von Null verschieden ist, z. B. die Zahl $\nu \cdot \mu_{n-1}'$, so läßt sich von neuem

$$\lambda' = \lambda'' + z_{n-1} \cdot \lambda_{n-1} \tag{50}$$

setzen, wenn unter

$$\lambda_{n-1} = y_1^{(n-1)} \mu_1' + y_2^{(n-1)} \mu_2' + \cdots + y_{n-1}^{(n-1)} \mu_{n-1}' \tag{51}$$

eine der letztgedachten Zahlen verstanden wird, bei welcher der letzte Koeffizient den kleinsten positiven Wert hat; und die Formel (50) gibt die sämtlichen der gesuchten Zahlen λ' und nur solche, wenn darin z_{n-1} alle rationalen ganzen Zahlen und λ'' alle Zahlen durchläuft, die zugleich im Modulus $[\mu_1', \mu_2', \cdots, \mu_{n-2}']$ und in $\mathfrak{m} - \mathfrak{m}'$ enthalten sind. Fährt man so fort und setzt die Ausdrücke für $\lambda', \lambda'', \cdots$ in die Gleichung (48) ein, so findet man offenbar zuletzt folgendes Resultat:

Alle Zahlen λ des Modulus $\mathfrak{m} - \mathfrak{m}'$ lassen sich darstellen in der Form:

$$\lambda = z_n \lambda_n + z_{n-1} \lambda_{n-1} + z_{n-2} \lambda_{n-2} + \cdots + z_1 \lambda_1, \tag{52}$$

in welcher die Koeffizienten z_i rationale ganze Zahlen, die λ_i aber in $\mathfrak{m} - \mathfrak{m}'$ enthaltene und durch Gleichungen von dieser Gestalt:

$$(53)\quad \begin{cases} \lambda_n = y_1^{(n)}\mu_1' + y_2^{(n)}\mu_2' + \cdots + y_{n-1}^{(n)}\mu_{n-1}' + y_n^{(n)}\mu_n' \\ \lambda_{n-1} = y_1^{(n-1)}\mu_1' + y_2^{(n-1)}\mu_2' + \cdots + y_{n-1}^{(n-1)}\mu_{n-1}' \\ \lambda_{n-2} = y_1^{(n-2)}\mu_1' + \cdots + y_{n-2}^{(n-2)}\mu_{n-2}' \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda_2 = y_1^{(2)}\mu_1' + y_2^{(2)}\mu_2' \\ \lambda_1 = y_1^{(1)}\mu_1' \end{cases}$$

bestimmte Zahlen sind; hier bedeuten die Koeffizienten $y_k^{(i)}$ ebenfalls ganze rationale Zahlen, unter denen insbesondere

$$y_n^{(n)},\ y_{n-1}^{(n-1)},\ \cdots,\ y_2^{(2)},\ y_1^{(1)}$$

positiv sind. Da nun auch jede in der Form (52) ausgedrückte Zahl mit den λ_i zugleich in $\mathfrak{m} - \mathfrak{m}'$ enthalten sein wird, so repräsentiert die Formel (52) den Modulus $\mathfrak{m} - \mathfrak{m}'$ selbst, und, weil die Determinante der Gleichungen (53) gleich

$$(54)\qquad y_1^{(1)} y_2^{(2)} \cdots y_{n-1}^{(n-1)} y_n^{(n)},$$

also von Null verschieden, demnach die λ_i unabhängige Zahlen jenes Modulus sind, so bilden diese letzteren eine Basis desselben.

Nun sei

$$\mu' = y_1\mu_1' + y_2\mu_2' + \cdots + y_n\mu_n'$$

irgend eine Zahl des Modulus $\mathfrak{m}'$. Da man setzen darf

$$y_n = y_n^{(n)} \cdot q_n + r_n,\quad 0 \overline{\gtrless} r_n < y_n^{(n)},$$

so zeigt der Ausdruck für λ_n, daß auch

$$\mu' = y_1'\mu_1' + \cdots + y_{n-1}'\mu_{n-1}' + r_n\mu_n' + q_n\lambda_n$$

geschrieben werden kann. Dieser Wert läßt sich ferner mittels des Ausdrucks für λ_{n-1} auf die folgende Form bringen:

$$\mu' = y_1''\mu_1' + \cdots + y_{n-2}''\mu_{n-2}' + r_{n-1}\mu_{n-1}' + r_n\mu_n' + q_{n-1}\lambda_{n-1} + q_n\lambda_n,$$

worin $0 \overline{\gtrless} r_{n-1} < y_{n-1}^{(n-1)}$ ist, usw., sodaß schließlich jeder Zahl μ' des Modulus $\mathfrak{m}'$ die Form gegeben werden kann:

$$\mu' = \lambda + r_1\mu_1' + r_2\mu_2' + \cdots + r_n\mu_n',$$

in welcher λ eine Zahl des Modulus $\mathfrak{m} - \mathfrak{m}'$ ist, die Koeffizienten r_i aber den Ungleichheiten

$$0 \overline{\gtrless} r_i < y_i^{(i)}$$
$$(\text{für } i = 1, 2, \cdots, n)$$

unterworfen sind; anders gesagt: jede Zahl in $\mathfrak{m}'$ ist einer ebenfalls in $\mathfrak{m}'$ enthaltenen Zahl

(55) $$r_1\mu_1' + r_2\mu_2' + \cdots + r_n\mu_n'$$

von der angegebenen Beschaffenheit der Koeffizienten r_i (mod. $\mathfrak{m} - \mathfrak{m}'$) kongruent. Die Anzahl solcher Zahlen ist offenbar

$$y_1^{(1)} \cdot y_2^{(2)} \cdots y_n^{(n)},$$

und sie sind alle (mod. $\mathfrak{m} - \mathfrak{m}'$) inkongruent; denn sonst müßte die Differenz zweier von ihnen:

$$(r_1'\mu_1' + r_2'\mu_2' + \cdots + r_n'\mu_n') - (r_1''\mu_1' + r_2''\mu_2' + \cdots + r_n''\mu_n'),$$

d. i. eine Zahl

$$\varrho_1\mu_1' + \varrho_2\mu_2' + \cdots + \varrho_n\mu_n'$$

mit Koeffizienten ϱ_i, die absolut kleiner sind als resp. $y_1^{(1)}$, $y_2^{(2)}, \cdots, y_n^{(n)}$ und deren letzter, wenn er nicht Null wäre, positiv vorausgesetzt werden darf, in $\mathfrak{m} - \mathfrak{m}'$ enthalten sein, gegen die Bedeutung der Zahl $y_n^{(n)}$; somit findet sich $\varrho_n = 0$, d. h. $r_n' = r_n''$ und nunmehr weiter durch analoges Schließen auch die Gleichheit von r_{n-1}' und r_{n-1}'', usw., kurz die Gleichheit der zwei Zahlen. Da zudem auch jede der Zahlen (55) in $\mathfrak{m}'$ enthalten ist, so folgt hieraus, daß dieselben ein vollständiges Restsystem von $\mathfrak{m}'$ (mod. $\mathfrak{m} - \mathfrak{m}'$) repräsentieren, und daß also

(56) $$(\mathfrak{m}', \mathfrak{m} - \mathfrak{m}') = (\mathfrak{m}', \mathfrak{m}) = y_1^{(1)} y_2^{(2)} \cdots y_n^{(n)}$$

ist.

Fassen wir diese verschiedenen Ergebnisse zusammen, so läßt sich folgender Satz aussprechen:

Hängen die Basen zweier n-gliedrigen Moduln $\mathfrak{m}$, $\mathfrak{m}'$ durch die Gleichungen (43) mit rationalen Koeffizienten c_{ik} zusammen, so ist ihr kleinstes gemeinsames Vielfache $\mathfrak{m} - \mathfrak{m}'$ ebenfalls ein n-gliedriger Modulus; dieser hat eine Basis $\lambda_1, \lambda_2, \cdots, \lambda_n$ von der Form der Ausdrücke (53), in denen die Koeffizienten $y_i^{(i)}$ positive ganze Zahlen sind, und das Produkt der letzteren ist gleich der Anzahl $(\mathfrak{m}', \mathfrak{m})$ der Klassen,

in welche die Zahlen des Moduls $\mathfrak{m}'$ sich (mod. $\mathfrak{m}$) verteilen.

Wir wollen nicht unterlassen darauf hinzuweisen, daß die Prämisse dieses Satzes allgemeiner gefaßt werden kann. Übersieht man noch einmal das Räsonnement, durch welches wir zu dem Satze geführt worden sind, so erkennt man, daß die vorausgesetzte Beziehung der beiden Moduln $\mathfrak{m}$, $\mathfrak{m}'$ zu einander und damit auch die Endlichkeit des Modulus $\mathfrak{m}$ nur insofern benutzt worden ist, als infolge derselben die Zahlen $\mu_1', \mu_2', \cdots, \mu_n'$ mit einer, von Null verschiedenen, rationalen (ganzen) Zahl multipliziert zugleich auch dem Modulus $\mathfrak{m}$ angehören. Das gesamte Räsonnement und der aus ihm gezogene Schlußsatz wird demnach bestehen bleiben, wenn seine Prämisse durch die allgemeinere ersetzt wird, daß die Elemente des n-gliedrigen Modulus $\mathfrak{m}'$ oder, was auf dasselbe hinauskommt, daß alle seine Zahlen durch Multiplikation mit, von Null verschiedenen, rationalen (ganzen) Zahlen in Zahlen des beliebigen Modulus $\mathfrak{m}$ verwandelt werden können.

Bleiben wir aber hier weiter bei der ursprünglichen Prämisse, so ist zu bemerken, daß dann auch die Elemente μ_i vermittelst der μ_i' durch lineare Gleichungen von derselben Beschaffenheit wie die Gleichungen (43) ausgedrückt werden können; daraus folgt dann aber, daß der Modulus $\mathfrak{m} - \mathfrak{m}'$ auch eine Basis $\varkappa_1, \varkappa_2, \cdots, \varkappa_n$ besitzt, deren Elemente durch nachstehende, den Gleichungen (53) völlig analog beschaffene Formeln bestimmt sind:

$$(57)\quad \begin{cases} \varkappa_n &= x_1^{(n)}\mu_1 + x_2^{(n)}\mu_2 + \cdots + x_{n-1}^{(n)}\mu_{n-1} + x_n^{(n)}\mu_n \\ \varkappa_{n-1} &= x_1^{(n-1)}\mu_1 + x_2^{(n-1)}\mu_2 + \cdots + x_{n-1}^{(n-1)}\mu_{n-1} \\ \cdot & \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot\quad \cdot \\ \varkappa_2 &= x_1^{(2)}\mu_1 + x_2^{(2)}\mu_2 \\ \varkappa_1 &= x_1^{(1)}\mu_1, \end{cases}$$

und daß die Determinante dieser Gleichungen, nämlich das Produkt $x_1^{(1)}x_2^{(2)} \cdots x_n^{(n)}$, gleich der Anzahl der Klassen ist, in welche die Zahlen von $\mathfrak{m}$ sich (mod. $\mathfrak{m}'$) verteilen:

$$(58)\qquad (\mathfrak{m}, \mathfrak{m}') = x_1^{(1)}x_2^{(2)} \cdots x_n^{(n)}.$$

Zwischen den Elementen $\varkappa_i$ der einen und den Elementen λ_i der anderen Basis des Modulus $\mathfrak{m} - \mathfrak{m}'$ bestehen aber Gleichungen von der Form:

$$\lambda_i = a_{i1}\varkappa_1 + a_{i2}\varkappa_2 + \cdots + a_{in}\varkappa_n, \quad (i = 1, 2, \cdots, n) \tag{59}$$

deren ganzzahlige Koeffizienten die Determinante ± 1 haben. Nun lassen sich die Elemente λ_i als lineare Funktionen der μ_i ausdrücken, indem man entweder in die Gleichungen (53) die Werte der μ_i' durch die Gleichungen (43), oder indem man in die Gleichungen (59) die Werte der $\varkappa_i$ durch die Gleichungen (57) einführt. Da beide Male die Determinante der erhaltenen Ausdrücke dieselbe sein muß, gibt der Multiplikationssatz für Determinanten mit Rücksicht auf die Formeln (56) und (58) nachstehende Gleichung:

$$(\mathfrak{m}', \mathfrak{m}) \cdot C = \pm 1 \cdot (\mathfrak{m}, \mathfrak{m}')$$

oder

$$\frac{(\mathfrak{m}, \mathfrak{m}')}{(\mathfrak{m}', \mathfrak{m})} = \pm C. \tag{60}$$

Hängen also die Basen zweier n-gliedrigen Moduln $\mathfrak{m}$, $\mathfrak{m}'$ durch die Gleichungen (43) mit rationalen Koeffizienten c_{ik} zusammen, so ist der Absolutwert der Determinante $C = |c_{ik}|$ gleich dem Verhältnisse der beiden Anzahlen $(\mathfrak{m}, \mathfrak{m}')$, $(\mathfrak{m}', \mathfrak{m})$. Sind insbesondere die Koeffizienten c_{ik} *ganze* rationale Zahlen, so ist der Absolutwert der Determinante $|c_{ik}|$ gleich der Anzahl $(\mathfrak{m}, \mathfrak{m}')$ der Klassen, in welche die Zahlen des Modulus $\mathfrak{m}$ sich (mod. $\mathfrak{m}'$) verteilen. Denn in diesem besonderen Falle ist der Modulus $\mathfrak{m}'$ in $\mathfrak{m}$ enthalten, alle seine Zahlen also kongruent Null (mod. $\mathfrak{m}$), mithin $(\mathfrak{m}', \mathfrak{m}) = 1$.

Drittes Kapitel.

Divisorensysteme. Höhere Kongruenzen.

1. Der Begriff eines endlichen Modulus gestattet eine wesentliche Modifikation oder Erweiterung, von der wir zwecks späterer Verwendung im Anschluß an die voraufgehenden Betrachtungen gleich hier handeln wollen.

Sind wieder $\mu_1, \mu_2, \cdots, \mu_n$ irgend welche gegebenen Größen, so bewahrt die Gesamtheit der aus der Linearform

$$(1) \qquad f = \mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n$$

hervorgehenden Größen den allgemeinen Charakter eines Modulus auch dann, wenn die Unbestimmten u_i, statt alle rationalen ganzen Zahlen anzunehmen, die sämtlichen rationalen Zahlen oder auch die Größen irgend eines bestimmten Rationalitätsbereiches $\mathfrak{R}$ oder auch nur die seines Integritätsbereiches durchlaufen. Wir heben aus diesen Fällen denjenigen hervor, wo die Elemente μ_i einem gegebenen Rationalitätsbereiche $\mathfrak{R}$ entnommen sind und die Unbestimmten u_i die *ganzen* Größen dieses Bereiches durchlaufen. In dieser Voraussetzung bezeichnen wir den entstehenden endlichen Modulus durch das Zeichen

$$\{\mu_1, \mu_2, \cdots, \mu_n\}$$

zum Unterschiede von dem Symbole

$$[\mu_1, \mu_2, \cdots, \mu_n],$$

welches nach wie vor den früheren endlichen Modulus anzeigen soll, der mittels rationaler ganzer Werte der Unbestimmten gebildet wird.

Ist also z. B. $\mathfrak{R}$ der Bereich R der rationalen Zahlen, so werden ersichtlich beide Symbole dieselbe Gesamtheit von Zahlen bezeichnen:

$$\{\mu_1, \mu_2, \cdots, \mu_n\} = [\mu_1, \mu_2, \cdots, \mu_n].$$

Bedeuten insbesondere $\mu_1, \mu_2, \cdots, \mu_n$ rationale *ganze* Zahlen, so reduziert sich, wie leicht zu sehen, dieser Modulus auf einen eingliedrigen Modulus. In der Tat, bedeutet d den größten gemeinsamen Teiler der Elemente $\mu_1, \mu_2, \cdots, \mu_n$, so wird für ganzzahlige Werte der u_i jede aus f entstehende Zahl ein Vielfaches von d, der ganze Modulus also im Modulus $[d]$ enthalten, mithin (nach Kap. 2, Nr. 4) von der Form $[hd]$ sein; da also unter allen seinen Zahlen auch seine Elemente Vielfache von hd sind, der größte gemeinsame Teiler derselben aber d ist, muß $h = 1$, folglich der Modulus gleich $[d]$ sein. Hieraus ist zugleich zu schließen, daß die unbestimmte Gleichung

$$\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n = d \tag{2}$$

in rationalen ganzen Zahlen auflösbar ist.

Der eingliedrige Modulus $[d]$, d. i. die Gesamtheit aller „durch d teilbaren" Zahlen du, erscheint durchaus geeignet, diesen „Teiler oder Divisor d" zu charakterisieren; zugleich ist sie die Klasse derjenigen Zahlen, welche (mod. d) der Null kongruent sind, und gibt so den Grund zu erkennen, aus welchem für jene Gesamtheit der Name Modulus gewählt worden ist. Es ist nur eine einfache Verallgemeinerung dieses Verhältnisses, wenn man nach Kroneckers Vorgange[1]) die ganzzahligen Elemente $\mu_1, \mu_2, \cdots, \mu_n$ des vorliegenden Modulus als ein „Divisorensystem" und seine Zahlen

$$\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_n u_n$$

als „die durch dasselbe teilbaren" Zahlen bezeichnet; die Verteilung aller Zahlen in Klassen kongruenter Zahlen in bezug auf ein solches System rechtfertigt dann die weitere Benennung des Divisorensystems auch als „eines Systems von Moduln". Diese Benennungen können wir dann aber auch auf den verallgemeinerten endlichen Modulus von der Art des Symbols

$$\{\mu_1, \mu_2, \cdots, \mu_n\}$$

unbedenklich übertragen.

Ist, um ein weiteres Beispiel zu betrachten, der Rationalitätsbereich, welchem die Elemente entnommen sind, der Bereich aller rationalen Funktionen einer Veränderlichen x mit beliebigen Zahlenkoeffizienten, sind also etwa

$$\mu_1 = f_1(x),\ \mu_2 = f_2(x),\ \cdots,\ \mu_n = f_n(x)$$

n gegebene Funktionen dieser Art, die wir indessen gleich als ganze Funktionen voraussetzen wollen, so wird der Modulus

$$\{f_1(x), f_2(x), \cdots, f_n(x)\} \tag{3}$$

die Gesamtheit aller Größen bedeuten von der Form

$$f_1(x)\varphi_1(x) + f_2(x)\varphi_2(x) + \cdots + f_n(x)\varphi_n(x), \tag{4}$$

worin die $\varphi_i(x)$ ebenfalls ganze Funktionen von x mit be-

---

1) L. Kronecker, Festschrift zu Herrn E. E. Kummers Doktor-Jubiläum 10. Sept. 1881.

liebigen Zahlenkoeffizienten bedeuten. Eine solche ganze Funktion $f(x)$ heiße Teiler einer anderen $F(x)$, wenn diese das Produkt aus $f(x)$ in eine ebenfalls ganze Funktion $\varphi(x)$ derselben Art ist,

$$F(x) = f(x) \cdot \varphi(x). \tag{5}$$

Zu den Teilern von $F(x)$ gehört, da

$$F(x) = r \cdot \frac{1}{r} F(x)$$

gesetzt werden kann, auch jede von Null verschiedene Zahl r, jede „Funktion nullten Grades“; und, ist $f(x)$ ein Teiler von $F(x)$, so ist's auch $r \cdot f(x)$. Unter allen solchen zusammengehörigen Teilern ist daher einer durch den Umstand ausgezeichnet, daß der Koeffizient des höchsten Gliedes gleich 1 ist; er soll ein primärer Teiler von $F(x)$ heißen. Die Anzahl dieser primären Teiler $f(x)$ ist offenbar endlich; denn jedem von ihnen entspricht eine Zerlegung (5) der Funktion $F(x)$, derzufolge die Wurzeln der beiden Faktoren zusammen diejenigen von $F(x)$ ausmachen; ist aber etwa m der Grad von $F(x)$, so ist 2^m die Anzahl der möglichen Verteilungen aller m Wurzeln in zwei Kategorieen, also ist auch die Anzahl der möglichen Zerlegungen in primäre Faktoren nur endlich. Jeder Teiler von $F(x)$ ist ersichtlich höchstens von gleichem Grade wie $F(x)$. Sind ferner $F(x)$, $f(x)$ irgend zwei Funktionen der gedachten Art, so liefert die algebraische Division der ersteren durch die zweite eine Gleichung von der Gestalt:

$$F(x) = f(x) \cdot q(x) + r(x), \tag{6}$$

worin $q(x)$, $r(x)$ wieder zwei ganze Funktionen von x derselben Art sind, deren letztere von geringerem Grade ist als $f(x)$. Man erkennt aus diesen Punkten ganz, wie bei dem vorigen Beispiele, daß jeder in einem eingliedrigen Modulus $\{f(x)\}$ enthaltene Modulus derartiger Funktionen ein Modulus von der Gestalt $\{q(x) \cdot f(x)\}$ ist, und auf Grund dieser Tatsache, indem man mit $f(x)$ einen allen Funktionen

$$f_1(x),\ f_2(x),\ \cdots,\ f_n(x)$$

gemeinsamen Teiler bezeichnet, dessen Grad am größten und welcher zugleich primär ist, die folgende Gleichheit:

$$\{f_1(x),\ f_2(x),\ \cdots,\ f_n(x)\} = \{f(x)\}. \tag{7}$$

Aus ihr ersieht man zugleich, daß die eben bezeichnete Funktion $f(x)$ eine eindeutig bestimmte ist; denn, gäbe es eine zweite $f'(x)$, so müßte jener Modulus auch gleich $\{f'(x)\}$ sein, was offenbar $f(x) = f'(x)$ zur Folge hätte. Diese so bestimmte Funktion $f(x)$ werde der größte, allen Funktionen $f_1(x), f_2(x), \cdots, f_n(x)$ gemeinsame Teiler genannt. Ist er eine primäre ganze Funktion nullten Grades, d. h. gleich Eins, so werden die Funktionen

$$f_1(x), f_2(x), \cdots, f_n(x),$$

indem man von den von x unabhängigen Teilern, d. i. von Zahlenfaktoren absieht, Funktionen ohne gemeinsamen Teiler, insbesondere, wenn es sich nur um zwei Funktionen $f_1(x), f_2(x)$ handelt, relativ prime Funktionen genannt. Alsdann gibt es ganze Funktionen $\varphi_1(x), \varphi_2(x), \cdots, \varphi_n(x)$ des gedachten Bereiches von der Beschaffenheit, daß die Gleichung besteht:

$$f_1(x)\varphi_1(x) + f_2(x)\varphi_2(x) + \cdots + f_n(x)\varphi_n(x) = 1, \tag{8}$$

in dem besonderen Falle zweier relativ primen Funktionen $f_1(x), f_2(x)$ mithin zwei ganze Funktionen $\varphi_1(x), \varphi_2(x)$ des Bereiches, für welche die Gleichung

$$f_1(x)\varphi_1(x) + f_2(x)\varphi_2(x) = 1 \tag{9}$$

erfüllt wird.

Hieraus folgt sogleich der fundamentale Satz:

Ein Produkt $f(x) \cdot f_1(x)$ zweier Funktionen, deren eine $f_1(x)$ relativ prim ist zu einer gegebenen Funktion $f_2(x)$ derselben Art, kann mit dieser nur dann einen Teiler gemeinsam haben, wenn der andere Faktor $f(x)$ des Produktes ihn hat; insbesondere kann das Produkt durch die gegebene Funktion nur dann teilbar sein, wenn dieser andere Faktor es ist. Durch Multiplikation der vorausgesetzten Gleichung (9) mit $f(x)$ geht nämlich die andere:

$$f(x)f_1(x) \cdot \varphi_1(x) + f_2(x) \cdot f(x)\varphi_2(x) = f(x)$$

hervor, aus welcher zu schließen ist, daß jeder gemeinsame Teiler von $f(x)f_1(x)$ und $f_2(x)$ auch aufgehen muß in $f(x)$; ist dieser gemeinsame Teiler also insbesondere $f_2(x)$ selbst, so muß in der Tat $f(x)$ teilbar sein durch $f_2(x)$.

Sind demnach beide Funktionen $f(x)$, $f_1(x)$ relativ prim zu $f_2(x)$, so kann auch ihr Produkt keinen Teiler mit $f_2(x)$ gemeinsam haben, d. h. das Produkt zweier Funktionen, deren jede relativ prim ist gegen eine gegebene Funktion, ist es gegen diese Funktion gleichfalls.

Auf diesen Sätzen beruht die Zerlegung jeder ganzen Funktion des gedachten Bereiches in ein Produkt von sogenannten Primfunktionen. Wir bezeichnen aber hier als Primfunktion jede primäre ganze Funktion von x mit beliebigen Zahlenkoeffizienten, welche nicht in das Produkt zweier (von x abhängigen) ganzen Funktionen derselben Art zerlegt werden kann. Ist nun eine ganze Funktion $F(x)$ desselben Bereiches nicht selbst eine Primfunktion oder nur durch einen Zahlenfaktor von einer solchen verschieden, so gibt es Teiler von $F(x)$ und unter ihnen einen oder mehrere von kleinstem Grade, die zudem primär gedacht werden dürfen; einer von diesen sei $P(x)$. Diese Funktion $P(x)$ ist sicher eine Primfunktion, denn, hätte sie einen von x abhängigen Teiler $f(x)$, so wäre letzterer auch ein Teiler von $F(x)$, aber gegen die Voraussetzung von kleinerem Grade wie $P(x)$. Hiernach kann man setzen

$$F(x) = P(x) \cdot F_1(x),$$

wo $F_1(x)$ wieder eine Funktion von der Art der Funktion $F(x)$, aber geringeren Grades wie sie ist. Wenn nun $F_1(x)$ noch keine Primfunktion oder von einer solchen nur durch einen Zahlenfaktor verschieden ist, so kann man in gleicher Weise

$$F_1(x) = P_1(x) \cdot F_2(x)$$

setzen, wo $P_1(x)$ eine Primfunktion, $F_2(x)$ aber eine ganze Funktion des Bereiches von kleinerem Grade ist als $F_1(x)$, und man hat somit jetzt

$$F(x) = P(x)\,P_1(x) \cdot F_2(x),$$

und kann in gleicher Weise fortschließen. Da aber die Grade der Funktionen $F(x), F_1(x), F_2(x), \cdots$ fort und fort abnehmen, so muß dieser Fortgang endlich zu einem Teiler $F_k(x)$ führen, der eine Primfunktion oder von einer solchen nur durch einen Zahlenfaktor verschieden ist, und es ergibt sich eine Zerlegung von $F(x)$ von der folgenden Gestalt:

$$(10) \qquad F(x) = c \cdot P(x) P_1(x) P_2(x) \cdots P_h(x),$$

in welcher c einen Zahlenfaktor, $P(x)$, $P_1(x)$, $P_2(x)$, $\cdots$, $P_h(x)$ aber lauter Primfunktionen bedeuten, die übrigens nicht voneinander verschieden zu sein brauchen. Der wesentliche Zusatz, den wir hierzu machen dürfen, daß eine solche Zerlegung von $F(x)$ eine eindeutige ist, beweist sich mittels der voraufgeschickten Sätze. Wäre nämlich

$$(11) \qquad F(x) = c' \cdot P'(x) P_1'(x) \cdots P_k'(x)$$

eine zweite gleichartige Zerlegung von $F(x)$, mithin

$$(12) \quad c \cdot P(x) P_1(x) \cdots P_h(x) = c' \cdot P'(x) P_1'(x) \cdots P_k'(x),$$

so müßte zugleich mit der linken die rechte Seite dieser Gleichung durch $P(x)$ teilbar sein. Da nun jede der Primfunktionen $P_i'(x)$, wenn sie nicht gleich $P(x)$ ist, relativ prim zu $P(x)$ sein muß, da sie außer sich selbst keinen (von x abhängigen) Teiler besitzt, so wäre das ganze Produkt zur Rechten prim gegen $P(x)$, also nicht durch $P(x)$ teilbar, wenn keine der Funktionen $P_i'(x)$ gleich $P(x)$ wäre. Man schließt mithin, daß eine derselben gleich $P(x)$ sein muß, und daß diese gleichen Faktoren aus beiden Seiten der Gleichung (12) sich heben. So müßten sämtliche Faktoren

$$P(x),\ P_1(x),\ \cdots,\ P_h(x)$$

der linken Seite sich heben, also $h \overline{\overline{<}} k$ sein; wäre aber $h < k$, so blieben dann rechts noch von x abhängige Faktoren, während die linke Seite sich auf die Konstante c reduzierte, was nicht sein kann; also ist $h = k$ und die einzelnen Funktionen zur Rechten denen zur Linken gleich; daraus folgt dann endlich auch $c = c'$, d. i. die völlige Identität der zweiten Zerlegung mit der ersten, w. z. b. w.

Faßt man schließlich die etwa gleichen Faktoren der Zerlegung immer zu einer Potenz zusammen, so läßt sich der folgende Satz aussagen, welcher dem Satze von der Zerlegung einer gewöhnlichen ganzen Zahl in Primfaktoren völlig entspricht: **Jede ganze Funktion $F(x)$ von x mit beliebigen Zahlenkoeffizienten kann auf eine und nur eine Weise als ein Produkt aus Potenzen von Primfunktionen derselben Art dargestellt werden in der Form:**

$$(13) \qquad F(x) = c \cdot P(x)^a \cdot P_1(x)^{a_1} \cdots P_k(x)^{a_k},$$

wo c einen Zahlenkoeffizienten, $a, a_1, \cdots, a_k$ positive ganze Zahlen bedeuten.

2. Man sieht leicht ein, daß, was hier für ganze Funktionen mit beliebigen Zahlenkoeffizienten gezeigt worden ist, auch Geltung behält, wenn man sich auf den Bereich ganzer Funktionen mit rationalen Koeffizienten beschränkt; die Primfunktionen bedeuten dann auch Funktionen dieses Bereiches und stimmen daher mit dem, was wir in Kap. 1 Nr. 5 irreduktible Funktionen genannt haben, überein. Anders aber verhält sich die Sache, wenn wir als den Bereich $\mathfrak{R}$, welchem die Elemente μ_i zu entnehmen sind, denjenigen der rationalen Funktionen von x mit ganzzahligen Koeffizienten und die Funktionen $f_i(x)$ als ganze Funktionen dieses Bereichs voraussetzen. Alsdann ist in der durch algebraische Division zu erhaltenden Gleichung (6) die Restfunktion $r(x)$ nicht immer eine ganze Funktion desselben Bereiches und die darauf beruhenden Schlußfolgerungen fallen dahin. In diesem Falle besteht mithin nicht immer eine Gleichheit (7), der gemäß sich der betrachtete Modulus auf einen eingliedrigen reduzierte, vielmehr zerfallen die Moduln

$$\{f_1(x), f_2(x), \cdots, f_n(x)\}$$

dieser neuen Art in zwei wesentlich verschiedene Kategorieen, welche Kronecker als Moduln erster und zweiter Stufe unterschieden hat: die der ersten lassen sich auf einen eingliedrigen Modulus reduzieren, die der anderen aber nicht.

Wir betrachten hier nur die Moduln von der Form

$$(14) \qquad \{p, f(x)\},$$

d. i. die Gesamtheit der Funktionen

$$(15) \qquad p\,\varphi(x) + f(x)\,\psi(x),$$

wo p eine Primzahl, $f(x)$ eine gegebene ganze, ganzzahlige Funktion von x, $\varphi(x)$ und $\psi(x)$ aber alle Funktionen dieser Art bedeuten.

Der einfachste von ihnen wäre der Modulus $\{p\}$, d. i. die Gesamtheit aller ganzen, ganzzahligen Funktionen $p \cdot \varphi(x)$, deren sämtliche Koeffizienten durch p teilbar sind.

Wir nennen zwei ganze, ganzzahlige Funktionen $f'(x), f''(x)$ nach diesem besonderen Modulus kongruent, in Zeichen:

$$f'(x) \equiv f''(x) \pmod{p},$$

wenn die Differenz $f'(x) - f''(x)$ eine Funktion des Modulus ist, nämlich die Koeffizienten gleich hoher Potenzen in $f'(x), f''(x)$ in gewöhnlichem Sinne (mod. p) kongruente Zahlen sind.

Für zwei solche kongruente Funktionen sind die Moduln

$$\{p, f'(x)\}, \quad \{p, f''(x)\}$$

ein und derselbe Modulus. Denn, ist

$$f'(x) - f''(x) = p \cdot \chi(x),$$

so wird

$$p\,\varphi(x) + f'(x)\,\psi(x) = p\,[\varphi(x) + \psi(x)\,\chi(x)] + f''(x)\,\psi(x),$$

wo nun, wenn $\varphi(x)$, $\psi(x)$ alle ganzen, ganzzahligen Funktionen bedeuten, dasselbe offenbar auch gilt von den Funktionen $\varphi(x) + \psi(x)\chi(x)$ und $\psi(x)$.

Hiernach darf man im Modulus (14) in der Funktion $f(x)$ alle Glieder unterdrücken, welche durch p teilbar sind; sind sie es sämtlich, also $f(x) \equiv 0 \pmod{p}$, so ist der Modulus (14) identisch mit dem Modulus $\{p\}$; ist dagegen m der **Grad der Funktion** $f(x)$ (mod. p), nämlich x^m das höchste der übrig bleibenden Glieder, also

$$f(x) \equiv cx^m + c_1 x^{m-1} + \cdots + c_{m-1}x + c_m \pmod{p}, \tag{16}$$

wo c nicht durch p aufgeht, so gibt es eine ganze Zahl c' derart, daß $cc' \equiv 1$ also

$$\left.\begin{aligned} cc' \cdot f(x) &\equiv f(x) \\ \text{und} \\ c'f(x) &\equiv x^m + c_1' x^{m-1} + \cdots + c_{m-1}' x + c_m' \quad (17) \end{aligned}\right\} \pmod{p}$$

ist; folglich ist nach dem Obigen

$$\{p, f(x)\} = \{p, cc'f(x)\}$$

und nun, wie ohne weiteres einleuchtet,

$$\{p, cc'f(x)\} \succ \{p, c'f(x)\} \succ \{p, f(x)\}$$

d. h.

$$\{p, f(x)\} = \{p, c'f(x)\}.$$

Man darf nach all' diesem im Modulus (14), wenn er von $\{p\}$ verschieden, die Funktion $f(x)$ von der Form

$$f(x) = x^m + c_1 x^{m-1} + \cdots + c_m \tag{18}$$

voraussetzen, in welcher der Koeffizient des höchsten Gliedes gleich 1, die der übrigen aber Zahlen aus der Reihe $0, 1, 2, \cdots, p-1$ sind. Jede Funktion von dieser Beschaffenheit werde primär genannt (mod. p); wird $f(x)$ als eine solche vorausgesetzt, so nennen wir den Modulus (14) reduziert.

Sind $f'(x)$, $f''(x)$ zwei (mod. p) primäre Funktionen von x, so folgt aus der Gleichheit

$$\{p, f'(x)\} = \{p, f''(x)\},$$

d. i. aus der Gleichheit zweier reduzierter Moduln von der Art (14) stets auch die Gleichheit ihrer Funktionen $f'(x)$, $f''(x)$. Denn der vorausgesetzten Gleichheit zufolge ist

$$f''(x) = p \cdot \varphi(x) + f'(x) \cdot \psi(x),$$

d. h.

$$f''(x) \equiv f'(x) \cdot \psi(x) \pmod{p};$$

gleichfalls aber ist

$$f'(x) = p \cdot \varphi'(x) + f''(x) \cdot \psi'(x),$$

d. h.

$$f'(x) \equiv f''(x) \cdot \psi'(x) \pmod{p}.$$

Aus beiden zusammen folgt

$$f''(x) \equiv f''(x) \cdot \psi(x) \psi'(x) \pmod{p},$$

eine Kongruenz, welche nur bestehen kann, wenn $\psi(x)$, $\psi'(x)$ vom Grade Null (mod. p), d. h. ganzen Zahlen c, c' kongruent sind, deren Produkt $cc' \equiv 1$ ist. Dann erfordert aber die Kongruenz

$$f''(x) \equiv c \cdot f'(x) \pmod{p},$$

daß beide Funktionen von gleichem Grade (mod. p) sind und daß, da die Koeffizienten ihrer höchsten Potenzen nach der Voraussetzung gleich 1, die übrigen kleiner als p sind,

$$c \equiv 1, \quad f''(x) \equiv f'(x) \pmod{p},$$

also sogar $f''(x) = f'(x)$ ist, wie behauptet.

Dies vorausgeschickt, zeigt sich sogleich, daß jeder Modulus (14), in welchem die Funktion $f(x)$ von

höherem als dem nullten Grade ist (mod. p), ein Modulus zweiter Stufe ist, es nämlich keine ganze ganzzahlige Funktion $\chi(x)$ gibt von der Beschaffenheit, daß

$$\{p, f(x)\} = \{\chi(x)\}$$

wäre. Denn, da alsdann sowohl p als auch $f(x)$ durch $\chi(x)$ teilbar sein würde, so müßte $\chi(x)$ gleich einer ganzen Zahl sein, durch welche die Funktion $f(x)$, da ihr höchster Koeffizient gleich 1, nicht teilbar sein kann, es sei denn, daß $\chi(x) = 1$. Dann aber müßte die Gleichung

$$p\,\varphi(x) + f(x)\,\psi(x) = 1,$$

d. h. die Kongruenz $f(x)\,\psi(x) \equiv 1 \pmod{p}$, welche, ausführlicher geschrieben, die Form

$$(x^m + c_1 x^{m-1} + \cdots + c_m) \cdot (b x^n + b_1 x^{n-1} + \cdots + b_n) \equiv 1$$

hätte, möglich sein, während sie doch unmöglich ist, da aus ihr der Reihe nach

$$b \equiv 0,\ b_1 \equiv 0,\ \cdots,\ b_n \equiv 0 \pmod{p}$$

im Widerspruch gegen den Wert der rechten Seite erschlossen wird.

Ist dagegen die Funktion $f(x)$ vom nullten Grade (mod. p) also, da sie von der Form (18) vorausgesetzt werden darf, $f(x) \equiv 1 \pmod{p}$, so wird der Modulus

$$\{p, f(x)\} = \{p, 1\} = \{1\},$$

d. i. gleich der Gesamtheit aller ganzen, ganzzahligen Funktionen von x sein. Der Modulus $\{p, f(x)\}$ möge ein eigentlicher Modulus heißen, wenn $f(x)$ von höherem als dem nullten Grade (mod. p), der Modulus also von der zweiten Stufe ist.

Wir beweisen nunmehr folgenden Satz: Sind

$$F_1(x),\ F_2(x),\ \cdots,\ F_n(x)$$

gegebene ganze, ganzzahlige Funktionen, unter denen wenigstens eine nicht kongruent Null ist (mod. p), und besteht die Beziehung

$$(19) \qquad \{p, F_1(x), F_2(x), \cdots, F_n(x)\} \succ \{p, f(x)\},$$

wo $\{p, f(x)\}$ einen beliebigen Modulus von der Art (14) bedeutet, so folgt daraus eine Gleichung von der Gestalt

(20) $\{p, F_1(x), F_2(x), \cdots, F_n(x)\} = \{p, f(x)\psi(x)\}$,

in welcher $\psi(x)$ eine (mod. p) primäre Funktion von x ist.

Bezeichnet nämlich $F(x)$ irgend eine in dem aus $n+1$ Elementen zusammengesetzten Modulus enthaltene Funktion, so besteht nach der Annahme eine Gleichung

$$F(x) = p\,\Phi(x) + f(x)\,\Psi(x)$$

oder eine Kongruenz

(21) $$F(x) \equiv f(x)\,\Psi(x) \pmod{p},$$

in welcher $\Psi(x)$ gewiß nicht $\equiv 0$ ist, wenn dies $F(x)$ nicht ist. Solche Funktionen $F(x)$ gibt es aber der Voraussetzung zufolge im Modulus; unter ihnen allen sei $F_0(x)$ eine derjenigen, bei denen der Grad der zugehörigen Funktion $\Psi(x)$, sie heiße $\Psi_0(x)$, deren Koeffizienten kleiner als p gedacht werden dürfen, am kleinsten ist. Wäre der Koeffizient b der höchsten Potenz in $\Psi_0(x)$ von 1 verschieden, so gäbe es eine Zahl b' derart, daß $bb' \equiv 1 \pmod{p}$, und durch Multiplikation der zugehörigen Kongruenz (21) mit b' erhielte man

(22) $$F^0(x) \equiv f(x)\,\Psi^0(x) \pmod{p},$$

wo $F^0(x) = b'F_0(x)$ eine ebenfalls in dem gedachten Modulus enthaltene Funktion, $\Psi^0(x)$ aber eine (mod. p) primäre Funktion von gleichem Grade wie $\Psi_0(x)$ ist. Da nun

$$\Psi(x) = Q(x) \cdot \Psi^0(x) + R(x)$$

gesetzt werden darf, wo $Q(x)$, $R(x)$ ganze, ganzzahlige Funktionen von x, die letztere von geringerem Grade wie $\Psi_0(x)$ bedeuten, erschließt man aus den Kongruenzen (21) und (22) diese andere:

$$F(x) - Q(x)\,F^0(x) \equiv f(x)\,R(x) \pmod{p},$$

wo die Funktion zur Linken ebenfalls dem gedachten Modulus angehört. Der Bedeutung der Funktion $\Psi_0(x)$ zufolge muß hier $R(x) \equiv 0$, folglich

$$F(x) \equiv Q(x) \cdot F^0(x) \pmod{p}$$

sein. Jede Funktion des aus den $n+1$ Elementen bestehenden Modulus ist — mit andern Worten — auch eine Funktion des Modulus

$$\{p, F^0(x)\} = \{p, f(x)\,\Psi^0(x)\};$$

da aber zugleich mit $F^0(x) \equiv f(x)\,\Psi^0(x)$ auch umgekehrt alle Funktionen des letztern Modulus in dem gedachten enthalten sind, so erhält man die Gleichheit beider Moduln, d. i. eine Beziehung von der zu erweisenden Form (20).

3. Bedeutet jetzt $F(x)$ eine der im Modulus (14) enthaltenen ganzen, ganzzahligen Funktionen, mithin

$$F(x) = p\,\varphi(x) + f(x)\,\psi(x) \tag{23}$$

oder auch

$$F(x) \equiv f(x)\,\psi(x) \pmod{p}, \tag{24}$$

so soll gesagt werden: $F(x)$ habe (mod. p) den Teiler $f(x)$. Man übersieht sogleich, daß die Teilbarkeit einer Funktion $F(x)$ durch eine andere Funktion $f(x)$ (mod. p) völlig gleichbedeutend ist mit dem Umstande, daß der Modulus $\{p, F(x)\}$ im Modulus $\{p, f(x)\}$ enthalten ist, d. i. mit der Teilbarkeit des ersteren Modulus durch den zweiten Modulus.

Da, wenn $F(x)$ nicht $\equiv 0$ (mod. p) ist, der Kongruenz (24) zufolge der dieser Funktion zukommende Grad M gleich der Summe der Grade von $f(x)$, $\psi(x)$ also mindestens gleich demjenigen von $f(x)$ ist, da ferner der Teiler $f(x)$ als primär (mod. p), d. i. von der Form (18) vorausgesetzt werden darf, so gibt es stets nur eine endliche Anzahl von verschiedenen primären Teilern einer gegebenen Funktion $F(x)$, denn die Anzahl der Funktionen (18), unter denen diese Teiler sich finden müssen, ist, da jeder der Koeffizienten c_i nur die p verschiedenen Werte $0, 1, 2, \cdots, p-1$ haben kann, m aber $\gtreqless M$ ist, höchstens gleich p^M. Denkt man sich daher jetzt n ganze, ganzzahlige Funktionen $F_1(x), F_2(x), \cdots, F_n(x)$ gegeben, unter denen wenigstens eine nicht kongruent Null ist (mod. p), so wird es wieder nur eine endliche Anzahl verschiedener primärer Funktionen $f(x)$ geben, welche gemeinsame Teiler derselben (mod. p) sind, derart, daß n Kongruenzen bestehen von der Form:

$$F_i(x) \equiv f(x)\cdot\psi_i(x) \pmod{p}; \quad (i = 1, 2, \cdots, n) \tag{25}$$

unter diesen primären gemeinsamen Teilern sei $f(x)$ einer von denjenigen, deren Grad (mod. p) am größten ist. Da den Kongruenzen (25) zufolge für die gedachten

Funktionen $F_i(x)$ die Beziehung (19) stattfindet, ergibt sich auch eine Gleichung von der Form (20), derzufolge sämtliche Funktionen $F_i(x)$ (mod. p) den gemeinsamen Teiler $f(x)\psi(x)$ hätten von höherem Grade wie $f(x)$, wenn nicht $\psi(x)$ von nulltem Grade also, als (mod. p) primäre Funktion, kongruent 1 (mod. p) wäre. Somit muß $\psi(x) \equiv 1$ (mod. p) sein und es ergibt sich die bestimmtere Gleichung

$$(26) \qquad \{p, F_1(x), F_2(x), \cdots, F_n(x)\} = \{p, f(x)\}.$$

Aus ihr erkennt man zugleich, daß der mit $f(x)$ bezeichnete, allen gegebenen Funktionen (mod. p) gemeinsame primäre Teiler höchsten Grades ein völlig bestimmter ist; denn, gäbe es noch einen zweiten $f'(x)$, so müßte der Modulus zur Linken von (26) auch gleich dem Modulus $\{p, f'(x)\}$ sein, woraus einem obigen Satze zufolge die Gleichheit der beiden Funktionen $f(x), f'(x)$ hervorginge. Demgemäß soll dieser Teiler $f(x)$ hinfort als der größte (mod. p) gemeinsame Teiler der gegebenen Funktionen bezeichnet werden.

Ist er gleich 1, so heißen die gegebenen Funktionen $F_1(x), F_2(x), \cdots, F_n(x)$ Funktionen ohne gemeinsamen Teiler (mod. p), insbesondere, wenn es sich nur um zwei Funktionen $F_1(x)$, $F_2(x)$ handelt, relativ prime Funktionen (mod. p). In diesem Falle gibt es ganze, ganzzahlige Funktionen $\varphi(x), \varphi_1(x), \varphi_2(x), \cdots, \varphi_n(x)$, für welche die Gleichung

$$p\,\varphi(x) + F_1(x)\,\varphi_1(x) + \cdots + F_n(x)\,\varphi_n(x) = 1$$

oder die Kongruenz

$$(27) \quad F_1(x)\,\varphi_1(x) + F_2(x)\,\varphi_2(x) + \cdots + F_n(x)\,\varphi_n(x) \equiv 1 \pmod{p}$$

erfüllt wird; mithin im Falle nur zweier (mod. p) relativ primen Funktionen $F_1(x)$, $F_2(x)$ zwei ganze, ganzzahlige Funktionen $\varphi_1(x)$, $\varphi_2(x)$ der Art, daß die Kongruenz stattfindet:

$$(28) \qquad F_1(x)\,\varphi_1(x) + F_2(x)\,\varphi_2(x) \equiv 1 \pmod{p}.$$

Wie nun aus der Gleichung (9) die Sätze über Teilbarkeit der ganzen Funktionen mit beliebigen bezw. rationalen Zahlenkoeffizienten erschlossen worden sind, genau ebenso ergeben sich aus der Kongruenz (28) völlig entsprechende Sätze über die Teilbarkeit (mod. p) der ganzen Funktionen mit ganzzahligen Koeffizienten. Multipliziert man nämlich (28) mit einer solchen Funktion $f(x)$, so daß die Kongruenz

$$(29)\quad f(x)F_1(x)\cdot\varphi_1(x)+F_2(x)\cdot f(x)\varphi_2(x)\equiv f(x)\ (\text{mod.}\,p)$$

hervorgeht, und nimmt an, $\varphi(x)$ sei ein den Funktionen $f(x)F_1(x)$ und $F_2(x)$ (mod. p) gemeinsamer Teiler derart, daß

$$f(x)F_1(x)\equiv\varphi(x)\psi_1(x),\quad F_2(x)\equiv\varphi(x)\psi_2(x)$$

gesetzt werden kann, so folgt aus (29)

$$f(x)\equiv\varphi(x)\cdot[\varphi_1(x)\psi_1(x)+f(x)\varphi_2(x)\psi_2(x)],$$

d. i. $\varphi(x)$ auch als ein Teiler von $f(x)$ (mod. p). Ein Produkt zweier ganzen, ganzzahligen Funktionen, deren eine (mod. p) relativ prim ist gegen eine gegebene Funktion derselben Art, kann also nur dann einen Teiler (mod. p) mit der letzteren gemeinsam haben, wenn der andere Faktor ihn hat; insbesondere kann das Produkt nur dann durch die gegebene Funktion teilbar sein (mod. p), wenn der andere Faktor es ist. Ist dagegen auch dieser relativ prim (mod. p) gegen die gegebene Funktion, so muß das Produkt es ebenfalls sein.

Wir definieren nun als Primfunktion (mod. p) eine Funktion $P(x)$, welche (mod. p) primär, also von der Beschaffenheit der Funktion (18) ist, und keinen von 1 und von ihr selbst verschiedenen primären Teiler (mod. p) besitzt.

Aus dieser Definition folgt sogleich der Satz: Eine Primfunktion $P(x)$ (mod. p) kann mit keiner Funktion $F(x)$ geringeren Grades einen Teiler (höheren als nullten Grades) (mod. p) gemeinsam haben, es sei denn, daß diese Funktion durch p teilbar ist. Denn, da dieser Teiler, welcher primär gedacht werden darf, nur $P(x)$ selbst sein könnte, so müßte eine Kongruenz bestehen von der Form

$$F(x)\equiv P(x)\cdot\psi(x)\ (\text{mod.}\,p),$$

worin $\psi(x)$ eine ganze, ganzzahlige Funktion bedeutet, was, da der Grad von $F(x)$ geringer ist als der von $P(x)$, erfordern würde, daß alle Koeffizienten von $\psi(x)$ und somit auch alle diejenigen von $F(x)$ durch p teilbar wären.

Jede Primfunktion $P(x)$ (mod. p) ist also (mod. p) relativ prim gegen ihre Ableitung $P'(x)$; denn sonst müßte $P'(x)\equiv 0$ (mod. p) sein, d. h., wenn

$$P(x) = x^f + c_1 x^{f-1} + \cdots + c_{f-1} x + c_f$$

gedacht wird, so müßten in

$$P'(x) = f \cdot x^{f-1} + c_1 (f-1) \cdot x^{f-2} + \cdots + 1 \cdot c_{f-1}$$

sämtliche Koeffizienten durch p teilbar sein; dies ergäbe $c_i \equiv 0 \pmod{p}$, wenn $f - i$ durch p nicht teilbar ist, und somit wäre

$$P(x) \equiv P_1(x^p) \equiv P_1(x)^p \pmod{p},[1]$$

wo $P_1(x)$ eine gewisse ganze, ganzzahlige Funktion bezeichnet, eine Folgerung, welche der Irreduktibilität der Funktion $P(x)$ (mod. p) widerstritte.

Denkt man sich ferner die endliche Anzahl primärer Teiler einer ganzen, ganzzahligen Funktion $F(x)$ (mod. p), unter denen der Teiler 1 der einzige von x unabhängige ist, so wird unter den übrigen wenigstens einer, er heiße $P(x)$, von kleinstem Grade (mod. p) sich finden, und dieser sicher eine Primfunktion (mod. p) sein müssen. Man darf also setzen

$$F(x) \equiv P(x) \cdot F_1(x) \pmod{p},$$

wo $F_1(x)$ wieder eine ganze, ganzzahlige Funktion ist, die nun ebenso (mod. p) in zwei Faktoren zerlegt werden kann, deren einer eine Primfunktion (mod. p) ist, usw. Auf diese Weise findet sich ganz entsprechend der Zerlegung (13) der ganzen Funktionen mit beliebigen bezw. rationalen Zahlenkoeffizienten die folgende Formel:

$$(30) \qquad F(x) \equiv c \cdot P(x)^a P_1(x)^{a_1} \cdots P_h(x)^{a_h} \pmod{p},$$

in welcher $P(x)$, $P_1(x)$, $\cdots$, $P_h(x)$ verschiedene Primfunktionen (mod. p), die Exponenten $a, a_1, \cdots, a_h$ positive ganze Zahlen und c den kleinsten positiven Rest bedeutet, welchen der Koeffizient des höchsten Gliedes in $F(x)$ (mod. p) läßt.

Die Eindeutigkeit dieser Zerlegung der Funktion $F(x)$ in ein Produkt von Primfunktionen (mod. p) ergibt sich schließlich genau ebenso, wie diejenige der Zerlegung (13), nämlich auf Grund der zuvor ausgesprochenen, den dortigen analogen, Teilbarkeitssätze.

---

1) S. Nr. 5, I.

Mittels der Formel (30) überzeugt man sich leicht, daß die Funktion $F(x)$ dann und nur dann einen gemeinsamen Teiler (mod. p) mit ihrer Ableitung $F'(x)$ besitzt, wenn sie wenigstens eine Primfunktion mehrfach zum Faktor hat. Man darf offenbar den gemeinsamen Teiler als Primteiler, z. B. als den Teiler $P(x)$, voraussetzen. Setzt man nun abkürzend

$$F(x) \equiv P(x)^a \cdot Q(x),$$

eine Formel, die mit einer Gleichung

$$F(x) = P(x)^a\, Q(x) + p \cdot f(x)$$

gleichbedeutend ist, in der auch $f(x)$ eine ganze, ganzzahlige Funktion bezeichnet, so kommt durch Differenzierung

$$F'(x) = P(x)^{a-1} \cdot Q_1(x) + p \cdot f'(x),$$

also

$$F'(x) \equiv P(x)^{a-1} \cdot Q_1(x) \text{ (mod. } p),$$

wo

$$Q_1(x) = a\, P'(x)\, Q(x) + P(x)\, Q'(x)$$

zu denken ist. Diese Funktion ist für $a = 1$ nicht durch $P(x)$ teilbar (mod. p), da die Funktion $Q(x)$ nach ihrer Bedeutung, $P'(x)$ aber dem oben Gezeigten gemäß relativ prim ist zu $P(x)$. Die Kongruenz für $F'(x)$ lehrt also, daß $F'(x)$ (mod. p) den Faktor $P(x)$ enthält oder nicht, jenachdem ihn $F(x)$ mehrfach oder einfach hat, wie behauptet.

4. Der Umstand, daß eine Funktion $F(x)$ dem Modulus $\{p, f(x)\}$ angehört oder eine Gleichung (23) oder die Kongruenz (24) stattfindet, läßt sich in einer noch vorteilhafteren Weise formulieren, indem man schreibt:

$$F(x) \equiv 0 \text{ mod. } \{p, f(x)\}. \tag{31}$$

Wir setzen aber hinfort $f(x)$ als eine Primfunktion $P(x)$ voraus, deren Grad wir n nennen. Für eine solche kann die Kongruenz

$$P(x) \equiv 0 \text{ (mod. } p) \tag{32}$$

keine ganzzahlige Wurzel haben, da sonst, wenn $x \equiv a$ eine wäre,

$$P(x) \equiv (x - a)\, P_1(x) \text{ (mod. } p)$$

gesetzt werden könnte, wo $P_1(x)$ eine ganze, ganzzahlige Funktion bedeutet, während doch $P(x)$ unzerlegbar ist (mod. p).

Nun werden wir später beweisen (Kap. 6, Nr. 3), daß eine ganze Funktion mit ganzzahligen Koeffizienten, deren höchster gleich 1, wenn sie nicht in zwei Faktoren mit ganzzahligen Koeffizienten zerlegbar ist, auch nicht in Faktoren mit rationalen Koeffizienten zerlegbar sein kann, mithin irreduktibel ist. Demnach muß die nach der Voraussetzung (mod. p) unzerlegbare Funktion $P(x)$ auch schlechthin irreduktibel sein, da aus einer Gleichung

$$P(x) = P_1(x) P_2(x),$$

in welcher dem Gesagten zufolge die Faktoren ganzzahlige Funktionen sein müßten, jedenfalls auch die Kongruenz

$$P(x) \equiv P_1(x) P_2(x) \pmod{p}$$

hervorginge, der Bedeutung von $P(x)$ zuwider. Hat nun zwar, wie bemerkt, die irreduktible Kongruenz (32) keine ganzzahlige Wurzel, so wird sie doch durch jede Wurzel α der irreduktibeln Gleichung

$$(33) \qquad P(x) = 0,$$

da für eine solche $P(\alpha)$ verschwindet, ebenfalls erfüllt sein, und α deshalb als eine, zwar nicht gewöhnliche, doch — um mit Galois[1]) zu reden, imaginäre Kongruenzwurzel eingeführt werden dürfen. Dann läßt sich zunächst einsehen, daß die Kongruenz

$$(34) \qquad F(x) \equiv 0 \mod. \{p,\ P(x)\}$$

völlig gleichbedeutend ist mit der anderen Kongruenz

$$(35) \qquad F(\alpha) \equiv 0 \pmod{p},$$

diese in dem Sinne einer Gleichung von der Gestalt

$$(36) \qquad F(\alpha) = p \cdot \varphi(\alpha)$$

und in ihr unter $\varphi(\alpha)$ eine ganze, ganzzahlige Funktion von α verstanden.

In der Tat, die Kongruenz (34) besagt, daß eine Gleichung besteht

$$(37) \qquad F(x) = p \cdot \varphi(x) + P(x) \cdot \psi(x)$$

1) E. Galois, Bulletin de Férussac 13, 1830, p. 398 und Journ. des Mathém. v. Liouville 11, 1846.

mit ganzen, ganzzahligen Funktionen $\varphi(x)$, $\psi(x)$, und aus ihr geht für $x = \alpha$ die Gleichung (36) oder die Kongruenz (35) hervor. Besteht aber umgekehrt die letztere, d. i. eine Gleichung (36), so folgt wegen der Irreduktibilität der Kongruenz (32), daß die Funktion

$$\mathrm{F}(x) = F(x) - p\varphi(x)$$

(mod. p) durch $P(x)$ teilbar sein muß; denn sonst wären $\mathrm{F}(x)$, $P(x)$ relativ prim (mod. p) und es bestände nach (28) eine Kongruenz von der Gestalt

$$\mathrm{F}(x) \cdot \varphi_1(x) + P(x) \cdot \varphi_2(x) \equiv 1 \pmod{p},$$

aus welcher für $x = \alpha$ die unmögliche andere

$$0 \equiv 1 \pmod{p}$$

hervorginge. Hiernach ergibt sich

$$F(x) - p\varphi(x) \equiv P(x) \cdot \psi(x) \pmod{p},$$

d. i. eine Gleichung von der Gestalt der Gleichung (37) oder die Kongruenz (34).

Hieraus folgt dann, daß α nicht Wurzel einer Kongruenz $F(x) \equiv 0 \pmod{p}$ geringeren als des n^{ten} Grades sein kann, es sei denn, daß diese identisch ist. Denn der Gleichung (37) zufolge müßte sonst

$$F(x) \equiv P(x)\,\psi(x) \pmod{p}$$

sein, was (s. vorige Nummer) unmöglich ist, wenn nicht alle Koeffizienten von $F(x)$ durch p teilbar sind. Es kann also eine Kongruenz

$$(38) \qquad a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \pmod{p}$$

mit ganzzahligen Koeffizienten nur stattfinden, wenn diese sämtlich durch p teilbar sind. Man darf daher in Analogie mit einer früheren Benennung sagen: die Potenzen

$$(39) \qquad 1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}$$

seien (mod. p) unabhängig von einander.

Betrachten wir nunmehr die Gesamtheit aller ganzen, ganzzahligen Funktionen

$$\omega = F(\alpha)$$

von α. Sie bilden einen Bereich von ganzen Größen — er heiße G_α — welche offenbar die Eigenschaft haben, durch Additionen, Subtraktionen und Multiplikationen einander zu reproduzieren. Da stets

$$F(x) = P(x)\,Q(x) + R(x)$$

gesetzt werden darf, wo $Q(x)$, $R(x)$ ganze Funktionen sind, die letztere von geringerem Grade als $P(x)$, deren Koeffizienten, da derjenige der höchsten Potenz in $P(x)$ gleich 1 ist, ganze Zahlen sein müssen, so ergibt sich auch die Kongruenz

$$(40)\qquad F(x) \equiv P(x)\,Q(x) + r(x) \pmod{p},$$

wenn unter $r(x)$ die Funktion verstanden wird, deren Koeffizienten die kleinsten nicht negativen Reste (mod. p) derjenigen von $R(x)$ sind. Dieser Kongruenz zufolge ist

$$F(\alpha) \equiv r(\alpha) \pmod{p},$$

d. h. jede Zahl $\omega = F(\alpha)$ des Bereiches G_α ist (mod. p) einem Ausdrucke kongruent von der Form

$$(41)\qquad r(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

dessen Koeffizienten a_i Zahlen aus der Reihe $0, 1, 2, \cdots, p-1$ sind.

Solcher Zahlen gibt es p^n und je zwei verschiedene von ihnen:

$$(42)\qquad \begin{array}{l} a_0' + a_1'\alpha + a_2'\alpha^2 + \cdots + a_{n-1}'\alpha^{n-1} \\ a_0'' + a_1''\alpha + a_2''\alpha^2 + \cdots + a_{n-1}''\alpha^{n-1} \end{array}$$

sind inkongruent (mod. p), denn sonst bestände eine Kongruenz (38), in welcher allgemein $a_i = a_i' - a_i''$ wäre, also müßten alle diese Differenzen kongruent Null (mod. p), oder vielmehr, da sie kleiner als p sind, gleich Null sein, was der Voraussetzung zuwider ist. Hiernach verteilen sich alle Zahlen ω des Bereichs G_α (mod. p) in p^n Klassen kongruenter Zahlen derart, daß zwei verschiedenen Klassen angehörige Zahlen unter einander inkongruent sind, und die p^n Zahlen von der Form (41) sind Repräsentanten dieser Klassen oder bilden ein vollständiges Restsystem für die Zahlen ω (mod. p). Eine einzige von ihnen, diejenige nämlich, deren Koeffizienten sämtlich Null sind, ist kongruent Null (mod. p).

Es gilt ferner der Satz: Das Produkt zweier Zahlen $F_1(\alpha)$, $F_2(\alpha)$ des Bereichs G_α ist nur dann kongruent Null (mod. p), wenn es einer der Faktoren ist. Denn aus

$$F_1(\alpha) \cdot F_2(\alpha) \equiv 0 \pmod{p}$$

fließt dem Obigen zufolge eine Kongruenz von der Form

$$F_1(x) \cdot F_2(x) \equiv P(x) \cdot \psi(x) \pmod{p},$$

d. h. die Primfunktion $P(x)$ ist ein Teiler des Produktes $F_1(x) \cdot F_2(x)$ (mod. p) und folglich auch eines seiner Faktoren, etwa ein Teiler von $F_1(x)$, dies aber zieht eine Kongruenz

$$F_1(\alpha) \equiv 0 \pmod{p}$$

nach sich, wie sie behauptet ist.

Dies vorausgeschickt, sei jetzt ω irgend eine Zahl des Bereiches G_α, welche nicht kongruent Null ist (mod. p), und man bezeichne zur Abkürzung mit ν die Potenz p^n und mit

$$(43) \qquad 0,\ \omega_1,\ \omega_2,\ \omega_3,\ \cdots,\ \omega_{\nu-1}$$

die p^n Repräsentanten (41) der inkongruenten Zahlenklassen oder allgemeiner irgend ein vollständiges Restsystem der Zahlen ω, d. i. ein System solcher Zahlen, die den Zahlen (41) bezw. kongruent sind. Dann sind auch die Produkte

$$(44) \qquad \omega \cdot 0,\ \omega\omega_1,\ \omega\omega_2,\ \omega\omega_3,\ \cdots,\ \omega\omega_{\nu-1}$$

einander (mod. p) inkongruent, da aus $\omega\omega_i \equiv \omega\omega_k$ sich die Kongruenz $\omega(\omega_i - \omega_k) \equiv 0$ und aus dieser, da ω nicht $\equiv 0$ ist, dem eben bewiesenen Satze gemäß sich $\omega_i \equiv \omega_k$ ergäbe gegen die Voraussetzung. Hierbei werden die beiden ersten Zahlen (43), (44) für sich kongruent sein. Da somit die übrigen Zahlen (44) den übrigen (43) insgesamt kongruent sind, so muß auch das Produkt derselben es dem Produkte der letzteren, also

$$\omega^{p^n-1} \cdot \omega_1\omega_2 \cdots \omega_{\nu-1} \equiv \omega_1\omega_2 \cdots \omega_{\nu-1} \pmod{p}$$

und, da das Produkt $\omega_1\omega_2 \cdots \omega_{\nu-1}$, dessen einzelne Faktoren nicht $\equiv 0$ sind, dies auch nicht sein kann, einfacher

$$(45) \qquad \omega^{p^n-1} \equiv 1 \pmod{p}$$

sein. Für jede Zahl ω des Bereiches G_α, welche nicht kongruent Null ist (mod. p), ist also die Kongruenz

(45) erfüllt, ein Satz, welcher ein Analogon des Fermatschen Satzes der gewöhnlichen Zahlentheorie bildet. Man gibt ihm sogleich eine andere Form, in welcher er für jede Zahl ω des Bereiches ohne Ausnahme gilt, indem man ihn ausspricht wie folgt: Jede Zahl ω des Bereiches G_α erfüllt die Kongruenz

$$(46) \qquad \omega^{p^n} \equiv \omega \pmod{p},$$

oder ist eine Wurzel der Kongruenz

$$(47) \qquad X^{p^n} \equiv X \pmod{p},$$

die somit genau ebensoviel Wurzeln im Bereiche G_α besitzt, als ihr Grad beträgt.

Hier gilt ferner ganz analog der gewöhnlichen Zahlentheorie der Satz, daß eine Kongruenz

$$(48) \qquad f(X) \equiv 0 \pmod{p},$$

in welcher $f(X)$ eine ganze Funktion von X vom Grade m mit zum Bereiche G_α gehörigen Koeffizienten bedeute, nicht mehr als m inkongruente Wurzeln in diesem Bereiche besitzen kann, es sei denn, daß sie identisch besteht. Hätte sie nämlich deren mindestens $m+1$, welche

$$\xi_0, \xi_1, \xi_2, \cdots, \xi_m$$

heißen mögen, so hätte die Kongruenz

$$f(X) - C \cdot (X - \xi_1)(X - \xi_2) \cdots (X - \xi_m) \equiv 0 \pmod{p},$$

deren Koeffizienten, wenn C denjenigen der höchsten Potenz von X in $f(X)$ bedeutet, wieder zum Bereiche G_α gehören, deren Grad aber nur noch $m-1$ sein kann, gewiß die m Wurzeln $\xi_1, \xi_2, \cdots, \xi_m$, sie müßte also identisch bestehen, wenn man den behaupteten Satz bereits für Kongruenzen des $m-1^{\text{ten}}$ Grades erwiesen annimmt. Aus der identischen Kongruenz

$$f(X) \equiv C \cdot (X - \xi_1)(X - \xi_2) \cdots (X - \xi_m) \pmod{p}$$

ergäbe sich dann aber für $X = \xi_0$ die Beziehung

$$0 \equiv C \cdot (\xi_0 - \xi_1)(\xi_0 - \xi_2) \cdots (\xi_0 - \xi_m) \pmod{p},$$

welche unmöglich ist, da nach der Voraussetzung keiner der Faktoren des rechtsstehenden Produktes kongruent Null (mod. p) ist. Der Satz gilt also für Kongruenzen m^{ten} Grades, wenn er

schon für Kongruenzen vom Grade $m-1$ besteht, und somit allgemein, da er offenbar für Kongruenzen ersten Grades richtig ist.

Verbindet man diesen allgemeinen Satz mit dem Analogon des Fermatschen Satzes, das wir erhielten, so darf man die nachstehende identische Kongruenz schreiben:

$$X^{p^n} - X \equiv X(X-\omega_1)(X-\omega_2)\cdots(X-\omega_{\nu-1}) \pmod{p},$$

oder einfacher

$$X^{p^n-1} - 1 \equiv (X-\omega_1)(X-\omega_2)\cdots(X-\omega_{\nu-1}) \pmod{p}, \tag{49}$$

aus welcher für $X=0$ die dem Wilsonschen Satze der gewöhnlichen Zahlentheorie entsprechende Beziehung

$$\omega_1\omega_2\cdots\omega_{\nu-1} \equiv -1 \pmod{p} \tag{50}$$

entspringt, sobald p eine ungerade Primzahl ist.

Endlich sei bemerkt, daß die Kongruenz (46), oder die nachstehende:

$$F(\alpha)^{p^n} \equiv F(\alpha) \pmod{p}$$

nach den oben gemachten Bemerkungen der anderen:

$$F(x)^{p^n} \equiv F(x) \quad \text{mod. } \{p,\ P(x)\}$$

völlig gleichbedeutend ist; demzufolge kann der verallgemeinerte Fermatsche Satz auch folgendermaßen ausgesprochen werden: Jede ganze ganzzahlige Funktion von x leistet der Kongruenz

$$X^{p^n} - X \equiv 0 \quad \text{mod. } \{p,\ P(x)\}$$

Genüge, welche Primfunktion n^{ten} Grades (mod. p) unter $P(x)$ auch verstanden werden mag.

5. Auf diesem Satze beruht die Zerlegung der Funktion

$$x^{p^m} - x$$

in ihre einfachsten Faktoren (mod. p); doch bedürfen wir, um sie und anderes herzuleiten, noch zweier einfachen Hilfssätze, die wir daher sogleich hier voraufschicken.

I. Ist

$$F(x) = ax^h + a_1x^{h-1} + \cdots + a_{h-1}x + a_h \tag{51}$$

eine ganze, ganzzahlige Funktion, so ist in bezug auf den Primzahlmodulus p stets

$$F(x)^p \equiv F(x^p) \pmod{p} \tag{52}$$

und daher allgemeiner für jeden positiven ganzen Exponenten n

$$F(x)^{p^n} \equiv F(x^{p^n}) \quad (\text{mod. } p). \tag{53}$$

In der Tat folgt bei Erhebung des Ausdrucks (51) zur p^{ten} Potenz nach der bekannten Eigenschaft des Polynomialkoeffizienten

$$F(x)^p \equiv a^p x^{hp} + a_1^p x^{(h-1)p} + \cdots + a_{h-1}^p x^p + a_h^p$$

und hieraus mit Rücksicht auf den Fermatschen Satz die Formel (52), aus welcher (53) durch wiederholte Potenzierung hervorgeht.

II. Ist ferner $\mathrm{F}(X)$ eine ganze, ganzzahlige Funktion von X und $X = F(x)$ eine Wurzel der Kongruenz

$$\mathrm{F}(X) \equiv 0 \quad \text{mod. } \{p,\ P(x)\}, \tag{54}$$

so sind die sämtlichen Potenzen

$$F(x),\ F(x)^p,\ F(x)^{p^2},\ F(x)^{p^3},\ \cdots \tag{55}$$

ebenfalls solche Wurzeln. Denn, besteht, wie die Voraussetzung ausspricht, eine Gleichung von der Form

$$\mathrm{F}(F(x)) = p \cdot \varphi(x) + P(x) \cdot \psi(x)$$

mit ganzen, ganzzahligen Funktionen $\varphi(x)$, $\psi(x)$, so folgt daraus, indem man die Unbestimmte x durch x^p ersetzt

$$\mathrm{F}(F(x^p)) = p \cdot \varphi(x^p) + P(x^p) \cdot \psi(x^p),$$

wofür dem ersten Hilfssatze zufolge offenbar auch geschrieben werden kann

$$\mathrm{F}(F(x)^p) = p \cdot \varphi_1(x) + P(x)^p \cdot \psi_1(x),$$

unter $\varphi_1(x)$, $\psi_1(x)$ wieder ganze, ganzzahlige Funktionen von x verstanden; es ist mithin

$$\mathrm{F}(F(x)^p) \equiv 0 \quad \text{mod. } \{p,\ P(x)\},$$

also $F(x)^p$ und ebenso dann auch jede der übrigen Potenzen (55) eine Wurzel der Kongruenz (54), wie behauptet.

Dies vorausgeschickt folgt nun zuerst aus dem verallgemeinerten Fermatschen Satze für jede Primfunktion $P(x)$ n^{ten} Grades (mod. p) die Kongruenz

$$x^{p^n} - x \equiv 0 \quad \text{mod. } \{p,\ P(x)\},$$

d. h. jede solche Primfunktion ist (mod. p) ein Primteiler von $x^{p^n} - x$.

Zweitens aber kann diese Differenz keinen Primteiler von höherem als dem n^{ten} Grade (mod. p) haben. Denn, wäre $P(x)$ ein solcher vom Grade $m > n$ also

$$x^{p^n} - x \equiv 0 \quad \text{mod.}\{p,\ P(x)\},$$

so bestünde auch für jede ganze, ganzzahlige Funktion $F(x)$ die Kongruenz

$$F(x^{p^n}) \equiv F(x) \quad \text{mod.}\ \{p,\ P(x)\}$$

und, da die (mod. p) erfüllte Kongruenz (53) a fortiori auch mod. $\{p,\ P(x)\}$ gelten muß, auch diese andere:

$$F(x)^{p^n} \equiv F(x) \quad \text{mod.}\ \{p,\ P(x)\};$$

da die Funktionen $F(x)$ aber in bezug auf den bezeichneten Doppelmodulus in genau $p^m > p^n$ inkongruente Klassen zerfallen, so hätte diese Kongruenz vom Grade p^n, was dem in voriger Nummer bewiesenen allgemeinen Kongruenzsatze zuwiderläuft, mehr als p^n Wurzeln.

Drittens können von den Primfunktionen $P(x)$, deren Grad $m < n$ ist, nur solche in $x^{p^n} - x$ aufgehen, für welche m ein Teiler von n ist. Wäre nämlich im Gegenteil $n = mq + r$, wo r positiv und kleiner als m ist, und wäre gleichwohl

$$x^{p^n} - x \equiv 0 \quad \text{mod.}\ \{p,\ P(x)\},$$

so ergäbe sich aus dem gleichzeitigen Bestehen dieser und der, dem allgemeinen Fermatschen Satze zufolge erfüllten Kongruenz

$$x^{p^m} - x \equiv 0 \quad \text{mod.}\ \{p,\ P(x)\}$$

leicht auch die dritte

$$x^{p^r} - x \equiv 0 \quad \text{mod.}\ \{p,\ P(x)\},$$

welche doch, da der Grad von $P(x)$ größer ist als r, nach dem eben Bewiesenen unmöglich ist.

Viertens geht dagegen jede Primfunktion $P(x)$, deren Grad ein Teiler d von n ist, in $x^{p^n} - x$ auf. Denn, da nach dem verallgemeinerten Fermatschen Satze

$$x^{p^d} - x \equiv 0 \quad \text{mod.}\ \{p,\ P(x)\}$$

sein muß, so folgt, wenn $n = qd$ gesetzt werden kann, offenbar auch

$$x^{p^n} - x \equiv 0 \quad \text{mod.}\ \{p,\ P(x)\}.$$

Endlich leuchtet aus der Identität

$$p^n \cdot (x^{p^n} - x) - x \cdot (p^n x^{p^n - 1} - 1) = x(1 - p^n)$$

sofort ein, daß die Funktion $x^{p^n} - x$ mit ihrer Abgeleiteten $p^n x^{p^n - 1} - 1$ keinen Teiler (mod. p) gemeinsam und daher auch keinen Teiler mehrfach besitzen kann.

Aus all' diesem, sowie aus dem Umstande, daß der höchste Koeffizient in $x^{p^n} - x$, wie in jeder Primfunktion (mod. p) gleich 1 ist, erschließt man dann die Zerlegung der Funktion $x^{p^n} - x$ in ihre Primfaktoren (mod. p), wie folgende Formel sie ausspricht:

$$(56) \qquad x^{p^n} - x \equiv \prod_{d:n} P_d'(x)\, P_d''(x) \cdots \quad (\text{mod.}\ p);$$

die Multiplikation ist hier auf alle verschiedenen Primfunktionen $P_d^{(i)}(x)$ (mod. p) zu erstrecken, deren Grad d gleich n oder ein Teiler von n ist.

Aus der Vergleichung der Grade beider Seiten dieser Kongruenz fließt zugleich die Formel

$$(57) \qquad p^n = \sum_{d:n} d \cdot (d),$$

welche ebenfalls über alle Teiler d von n, diese Zahl einschließlich, erstreckt zu denken ist, während (d) die Anzahl der verschiedenen Primfunktionen d^{ten} Grades (mod. p) bedeutet. Auf Grund eines allgemeinen zahlentheoretischen Satzes (s. Elemente der Zahlentheorie, S. 41) ergibt sich aus ihr diese andere:

$$(58) \qquad n \cdot (n) = p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \cdots,$$

worin die erste Summe auf alle Primfaktoren a von n, die zweite auf alle Kombinationen a, b je zweier derselben usw. ausgedehnt werden muß. Da der Ausdruck zur Rechten offenbar nicht Null werden kann, geht aus der Formel die wichtige Folgerung hervor: daß (mod. p) Prim-

funktionen jeden beliebigen Grades immer vorhanden sind; die Anzahl derjenigen vom Grade n ist

$$(59)\qquad (n) = \frac{p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \cdots}{n}.$$

Derselbe zahlentheoretische Satz liefert auch das Produkt aller dieser Primfunktionen n^{ten} Grades. Setzt man nämlich das Produkt der Primfunktionen d^{ten} Grades

$$P_d'(x) P_d''(x) \cdots = \Phi_d(x)$$

und

$$(60)\qquad \prod_{d:n} \Phi_d(x) = \Psi_n(x),$$

mithin

$$\sum_{d:n} \log \cdot \Phi_d(x) = \log \cdot \Psi_n(x),$$

so geht hieraus jenem Satze zufolge die Formel

$$\log \cdot \Phi_n(x) = \log \cdot \Psi_n(x) - \sum \log \cdot \Psi_{\frac{n}{a}}(x) + \sum \log \cdot \Psi_{\frac{n}{ab}}(x) - \cdots$$

hervor, der man die gleichbedeutende

$$\Phi_n(x) = \frac{\Psi_n(x) \cdot \prod \Psi_{\frac{n}{ab}}(x) \cdots}{\prod \Psi_{\frac{n}{a}}(x) \cdot \prod \Psi_{\frac{n}{abc}}(x) \cdots}$$

substituieren kann. Indem man hier aber mit dem Nenner multipliziert und die Formeln (56) und (60) in Betracht zieht, erhält man die Beziehung

$$(61)\quad \Phi_n(x) \cdot \prod \left(x^{p^{\frac{n}{a}}} - x\right) \cdots \equiv \left(x^{p^n} - x\right) \cdot \prod \left(x^{p^{\frac{n}{ab}}} - x\right) \cdots (\text{mod.}\, p).$$

Da nun, wie man sich unschwer überzeugt (s. des Verfassers „Niedere Zahlentheorie". Lpzg. 1902, S. 381, 382), der Ausdruck

$$\frac{\left(x^{p^n} - x\right) \cdot \prod \left(x^{p^{\frac{n}{ab}}} - x\right) \cdots}{\prod \left(x^{p^{\frac{n}{a}}} - x\right) \cdot \prod \left(x^{p^{\frac{n}{abc}}} - x\right) \cdots}$$

einer ganzen, ganzzahligen Funktion gleich ist und da in (61) die Funktion $\Phi_n(x)$ mit einer ebensolchen Funktion multipliziert ist, deren höchster Koeffizient zudem die Einheit ist, ergibt

sich daraus sogleich die verlangte Darstellung für das Produkt aller Primfunktionen n^{ten} Grades mittels der Formel

$$(62)\quad \Phi_n(x) \equiv \frac{(x^{p^n} - x)\cdot \prod (x^{p^{\frac{n}{ab}}} - x)\cdots}{\prod (x^{p^{\frac{n}{a}}} - x)\cdot \prod (x^{p^{\frac{n}{abc}}} - x)\cdots} \pmod{p},$$

in welcher die Ausdehnung der einzelnen Produkte die gleiche ist, wie die der einzelnen Summen in der Formel (58).

Man kann schließlich diesen Formeln eine bequemere einfache Gestalt geben, wenn man sich eines Funktionszeichens bedient, welches Kronecker eingeführt hat. Man verstehe für jeden Teiler d von n unter dem Zeichen ε_d die Null, wenn $\frac{n}{d}$ irgend welche gleiche Faktoren enthält, im entgegengesetzten Falle die Eins, diese aber positiv oder negativ genommen, jenachdem die Anzahl der Primfaktoren von $\frac{n}{d}$ gerade oder ungerade ist. Unter dieser Übereinkunft lassen sich die Formeln (59) und (62) folgendermaßen schreiben:

$$(63)\quad \begin{aligned} n\cdot(n) &= \sum_{d:n} \varepsilon_d p^d \\ \Phi_n(x) &\equiv \prod_{d:n} (x^{p^d} - x)^{\varepsilon_d} \pmod{p}. \end{aligned}$$

6. Nun wird nach dem Obigen die Kongruenz

$$x^{p^n} - x \equiv 0 \pmod{p}$$

von den sämtlichen Zahlen ω des Bereiches G_α erfüllt und diese zerfallen in p^n (mod. p) inkongruente Klassen. Wegen Formel (56) verteilen sich daher die p^n in G_α möglichen Wurzeln jener Kongruenz auf die verschiedenen Faktoren $P_d^{(i)}(x)$ der rechten Seite dieser Formel in der Art, daß jeder genau soviel Wurzeln hat, als sein Grad angibt, da sonst gegen den früher bewiesenen allgemeinen Kongruenzsatz einer von ihnen mehr Wurzeln zulassen müßte, als sein Grad beträgt. Es bleibt jedoch noch zu untersuchen, welche der p^n

möglichen Wurzeln einem jeden dieser Faktoren zukommen. Um diese Frage zu erledigen, stellen wir nachfolgende Betrachtungen an, denen auch sonst ein Interesse zukommt.

Jede Zahl ω in G_α, welche nicht kongruent Null (mod. p) ist, erfüllt die Kongruenz

$$\omega^{p^n-1} \equiv 1 \pmod{p}, \tag{64}$$

es kann aber sein, daß schon eine niedrigere Potenz von ω den gleichen Rest (mod. p) läßt. Ist nun ω^δ die niedrigste Potenz dieser Art, so nennen wir $\delta > 0$ den Exponenten, zu welchem ω (mod. p) *gehört*. Da alsdann außer (64) auch die Kongruenz

$$\omega^\delta \equiv 1 \pmod{p} \tag{65}$$

besteht, findet sich leicht, daß δ ein Teiler von $p^n - 1$ sein muß, denn, wäre im Gegenteil $p^n - 1 = q\delta + r$, wo r positiv und kleiner als δ, so erschlösse man aus (64) und (65) auch

$$\omega^r \equiv 1 \pmod{p}$$

gegen die Bedeutung des Exponenten δ. Sei nun δ irgend ein bestimmter Teiler von $p^n - 1$. Da dann

$$x^{p^n-1} - 1 = (x^\delta - 1) \cdot Q(x)$$

gesetzt werden kann, unter $Q(x)$ eine ganze, ganzzahlige Funktion verstanden, und da die linke Seite dieser Formel (mod. p) genau soviel Wurzeln in G_α hat, als ihr Grad aussagt, nämlich die $p^n - 1$ (mod. p) inkongruenten Zahlen ω, welche nicht kongruent Null sind, so muß auch die Kongruenz

$$x^\delta - 1 \equiv 0 \pmod{p} \tag{66}$$

genau δ solche Wurzeln in G_α besitzen. Jede derselben gehört zu einem bestimmten Exponenten t (mod. p), der wieder, wie aus dem gleichzeitigen Bestehen der Kongruenzen

$$\omega^\delta \equiv 1, \ \omega^t \equiv 1 \pmod{p}$$

zu erschließen ist, ein Teiler von δ sein muß; wie denn auch umgekehrt jede zum Teiler t von δ gehörige Zahl eine der δ Wurzeln von (66) sein wird. Nennt man daher $\gamma(t)$ die Anzahl aller inkongruenten zum Exponenten t gehörigen Zahlen, so ergibt sich ohne weiteres die Beziehung

$$\sum_{t:\delta} \gamma(t) = \delta,$$

aus welcher nach dem schon zweimal benutzten zahlentheoretischen Satze sich der Wert der Funktion $\gamma(\delta)$ ergibt, nämlich gleich der bekannten zahlentheoretischen Funktion $\varphi(\delta)$, welche durch die gleiche Formel

$$\sum_{t:\delta} \varphi(t) = \delta$$

bestimmt wird, also

$$\gamma(\delta) = \varphi(\delta) \tag{67}$$

(für jeden Teiler δ von $p^n - 1$).

Dieser Formel zufolge sind, was bisher noch fraglich scheinen durfte, für jeden Teiler δ von $p^n - 1$ wirklich Zahlen vorhanden, die zu ihm gehören.

Haben wir in dieser Weise alle Zahlen ω des Bereiches G_α, welche nicht kongruent Null sind (mod. p), nach dem Exponenten δ, zu welchem sie gehören, in Klassen von je $\varphi(\delta)$ Zahlen verteilt, so wollen wir dieser Verteilung jetzt eine andere an die Seite stellen, und dann beide Verteilungen mit einander vergleichen. Jede Zahl ω erfüllt die Bedingung

$$\omega^{p^n} \equiv \omega \quad (\text{mod. } p), \tag{68}$$

aber es ist möglich, daß n nicht die kleinste positive Zahl ist, für welche eine Kongruenz dieser Gestalt besteht. Ist dann d für eine Zahl ω die kleinste positive Zahl, für welche

$$\omega^{p^d} \equiv \omega \quad (\text{mod. } p) \tag{69}$$

ist, so soll gesagt werden, die Zahl ω *passe* zum Exponenten d. Man erkennt sogleich, daß d ein Teiler von n sein muß. Denn, wäre im Gegenteil $n = qd + r$, wo r positiv und kleiner als d, so ergäbe sich aus (69) durch wiederholte Erhebung zur Potenz p^d die Kongruenz

$$\omega^{p^{qd}} \equiv \omega,$$

folglich

$$\omega^{p^n} \equiv \omega^{p^r},$$

mithin gegen die Bedeutung des Exponenten d schon

$$\omega^{p^r} \equiv \omega \pmod{p}.$$

Sei jetzt d irgend ein bestimmter Teiler von n. Da dann auch $p^n - 1$ teilbar ist durch $p^d - 1$, so geht die Funktion $x^{p^n-1} - 1$ durch $x^{p^d-1} - 1$ auf und folglich kann man

$$x^{p^n} - x = (x^{p^d} - x) \cdot Q(x)$$

setzen, wo $Q(x)$ eine ganze, ganzzahlige Funktion bedeutet. Weil nun die linke Seite jede der p^n (mod. p) inkongruenten Zahlen ω zur Wurzel hat, muß auch die Kongruenz

$$x^{p^d} - x \equiv 0 \pmod{p} \tag{70}$$

genau p^d Wurzeln in G_α besitzen. Jede derselben aber paßt zu einem bestimmten Exponenten t, der wieder sogleich aus dem gleichzeitigen Bestehen der Kongruenzen

$$\omega^{p^d} \equiv \omega, \quad \omega^{p^t} \equiv \omega \pmod{p}$$

als ein Teiler von d erkannt wird; und umgekehrt wird jede zu einem Teiler t von d passende Zahl auch eine Wurzel der Kongruenz (70) sein, so daß sich folgende Beziehung aussagen läßt:

$$\sum_{t:d} g(t) = p^d, \tag{71}$$

in welcher mit $g(t)$ die Anzahl der zum Exponenten t passenden inkongruenten Zahlen ω bezeichnet ist. Vergleicht man diese Formel aber mit der Formel (57), so erschließt man dem zahlentheoretischen Hilfssatze zufolge die Gleichung

$$g(d) = d \cdot (d), \tag{72}$$

(für jeden Teiler d von n)

welche auch hier wieder lehrt, daß in jeder der Klassen, in welche wir jetzt die Zahlen ω nach dem Exponenten, zu welchem sie passen, verteilt haben, wirklich Zahlen vorhanden sind.

Betrachten wir insbesondere die Klasse der zum Exponenten 1 passenden Zahlen ω, d. h. die Wurzeln der Kongruenz

$$x^p \equiv x \pmod{p}. \tag{73}$$

Da diese durch jede der Zahlen $0, 1, 2, \cdots, p-1$ erfüllt wird, welche nicht nur im gewöhnlichen, sondern, wie leicht

einzusehen, auch im Sinne der Kongruenz (35) inkongruent sind, und da sie zudem nicht mehr als p Würzeln in $\mathfrak{G}_a$ haben kann, so ergibt sich, daß jede Zahl ω, welche die Kongruenz (73) erfüllt, einer der Zahlen

$$0, 1, 2, \cdots, p-1 \pmod{p}$$

kongruent sein muß.

7. Um nun festzustellen, wie die besprochenen beiden Verteilungen der Zahlen ω in Klassen einmal nach dem Exponenten, zu dem sie gehören, das andere Mal nach demjenigen, zu welchem sie passen, sich zueinander verhalten, bemerke man vor allem, daß, wenn eine Zahl ω, welche nicht kongruent Null ist (mod. p), zum Exponenten d paßt, die Kongruenz (69) einfacher auch so geschrieben werden kann:

$$\omega^{p^d-1} \equiv 1 \pmod{p} \tag{74}$$

und daß somit ω nur zu einem Exponenten δ_d gehören kann, der ein Teiler ist von p^d-1. Derselbe Exponent kann aber kein Teiler eines ähnlichen Ausdrucks p^e-1 sein, in welchem $0<e<d$ ist; denn mit der Kongruenz $\omega^{\delta_d} \equiv 1$ bestände dann auch die Kongruenz

$$\omega^{p^e-1} \equiv 1, \tag{75}$$

also auch, der über ω gemachten Annahme entgegen, diese andere:

$$\omega^{p^e} \equiv \omega \pmod{p}.$$
$$(0<e<d)$$

Aus diesem Grunde nennen wir δ_d einen dem Ausdrucke p^d-1 **eigenen** Teiler und dürfen dann als Resultat unserer bisherigen Betrachtung den Satz aussprechen: Jede zum Exponenten *d passende* Zahl ω, welche nicht kongruent Null ist (mod. p), *gehört* zu einem dem Ausdrucke p^d-1 *eigenen* Teiler δ_d. Und auch umgekehrt. Denn, ist δ_d ein solcher Teiler und gehört ω zum Exponenten δ_d, so folgt aus $\omega^{\delta_d} \equiv 1$ auch die Kongruenz (74), mithin auch $\omega^{p^d} \equiv \omega$; paßte nun ω nicht zu d, so müßte eine Kongruenz $\omega^{p^e} \equiv \omega$ bestehen, in welcher der Exponent $e<d$ sein müßte, woraus dann die Kongruenz (75) und δ_d als ein Teiler von p^e-1 hervorginge gegen die Voraussetzung. Aus diesem Ergebnisse

schließt man aber sogleich weiter, daß, wenn man mit $\delta_d', \delta_d'', \delta_d''', \cdots$ die verschiedenen dem Ausdrucke p^d-1 eigenen Teiler bezeichnet, die gesamte Klasse der zu *d passenden* Zahlen ω (welche nicht $\equiv 0 \pmod{p}$ sind) aus den Klassen der zu jenen Teilern $\delta_d', \delta_d'', \delta_d''', \cdots$ *gehörigen* Zahlen zusammengesetzt ist.

Ist nun ω eine zum Exponenten $\delta_d^{(h)}$ gehörige Zahl, so ist jede der Potenzen $\omega^p, \omega^{p^2}, \omega^{p^3}, \cdots$ es ebenfalls. Denn erstens folgt aus $\omega^{\delta_d^{(h)}} \equiv 1$ auch

$$\left(\omega^{p^k}\right)^{\delta_d^{(h)}} \equiv 1,$$

aber es kann auch keine kleinere Potenz von ω^{p^k} kongruent 1 sein, weil umgekehrt aus $\left(\omega^{p^k}\right)^t \equiv 1$ der Exponent $p^k \cdot t$ und, da p^k zu p^d-1 mithin auch zum Teiler $\delta_d^{(h)}$ von p^d-1 prim ist, auch t durch $\delta_d^{(h)}$ teilbar befunden würde. Unter jenen Potenzen sind die d folgenden:

$$\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}} \tag{76}$$

(mod. p) inkongruent, da aus der Kongruenz zweier derselben:

$$\omega^{p^k} \equiv \omega^{p^{k'}} \pmod{p},$$

worin etwa $k' > k$ sei, durch Erhebung in die Potenz p^{d-k} und mit Rücksicht auf (69)

$$\omega^{p^{k'-k}} \equiv \omega \pmod{p}$$

hervorginge, während doch $k'-k < d$ ist. Die nun folgenden Potenzen $\omega^{p^d}, \omega^{p^{d+1}}, \cdots$ sind wegen (69) den ersten d Potenzen periodisch kongruent. Die Gruppen aber, welche zwei zum Exponenten $\delta_d^{(h)}$ gehörigen Zahlen ω, ω' entsprechen,

$$\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}$$

$$\omega', \omega'^p, \omega'^{p^2}, \cdots, \omega'^{p^{d-1}},$$

sind (mod. p) inkongruent, wenn nicht ω' schon in der ersten enthalten ist, denn aus

$$\omega^{p^k} \equiv \omega'^{p^{k'}} \pmod{p}$$

erschließt man leicht

$$\omega' \equiv \omega^{p^h} \pmod{p},$$

wo h der kleinste positive Rest von $d+k-k'$ (mod. d).

Demnach zerfällt die ganze Klasse der $\varphi(\delta_d^{(h)})$ zum Exponenten $\delta_d^{(h)}$ gehörigen Zahlen in

$$\varphi_d^{(h)} = \frac{\varphi\left(\delta_d^{(h)}\right)}{d}$$

Unterabteilungen von je d Zahlen (76).

Die d der i^{ten} dieser Unterabteilungen angehörigen Zahlen sind immer die Wurzeln einer ganzen, ganzzahligen und (mod. p) irreduktibeln Kongruenz d^{ten} Grades

$$P_d^{(i)}(x) \equiv 0 \pmod{p}. \tag{77}$$

In der Tat leisten sie einer Kongruenz von der Form

$$(x-\omega)(x-\omega^p)\left(x-\omega^{p^2}\right)\cdots\left(x-\omega^{p^{d-1}}\right) \equiv 0$$

Genüge, deren Koeffizienten die einfachsten ganzen und ganzzahligen symmetrischen Funktionen von $\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}$ sind. Ist aber

$$S\left(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}\right)$$

irgend eine solche Funktion, so findet sich nach dem ersten Hilfssatze

$$S\left(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}\right)^p \equiv S\left(\omega^p, \omega^{p^2}, \omega^{p^3}, \cdots, \omega^{p^d}\right),$$

d. i. mit Rücksicht auf (69) und wegen der Symmetrie der Funktion S die Kongruenz

$$S\left(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}\right)^p \equiv S\left(\omega, \omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}\right),$$

mithin leistet die zu G_α gehörige Größe S der Kongruenz (73) Genüge und ist daher nach der an diese geknüpften Bemerkung einer ganzen Zahl (mod. p) kongruent. Daß die ganzzahlige Kongruenz (77) aber auch (mod. p) irreduktibel ist, ergibt sich mittels des zweiten Hilfssatzes. Wäre nämlich

$$P_d^{(i)}(x) \equiv \varphi(x)\,\psi(x) \pmod{p},$$

unter $\varphi(x)$, $\psi(x)$ ganze, ganzzahlige Funktionen verstanden, so müßte die Zahl ω, da sie eine Wurzel der linken Seite ist, auch etwa der Kongruenz

$$\varphi(x) \equiv 0 \pmod{p}$$

genügen, deren Grad kleiner ist als d. Dann würde aber die letztere Kongruenz nach jenem Hilfssatze auch die Wurzeln

$\omega^p, \omega^{p^2}, \cdots, \omega^{p^{d-1}}$ haben müssen, was wegen ihres Grades nicht angeht.

Hiernach sind die $\varphi(\delta_d^{(h)})$ zum Exponenten $\delta_d^{(h)}$ gehörigen Zahlen zusammengenommen die Wurzeln der Kongruenz

$$\prod_i P_d^{(i)}(x) \equiv 0 \text{ (mod. } p),$$

in welcher die Multiplikation über die Werte $i = 1, 2, \cdots, \varphi_d^{(h)}$ erstreckt zu denken ist; desgleichen werden daher die sämtlichen zum Exponenten d passenden Zahlen, welche nicht kongruent Null sind (mod. p), die Wurzeln der Kongruenz

$$\prod_h \prod_i P_d^{(i)}(x) \equiv 0 \text{ (mod. } p)$$

sein, wo in der zweiten Multiplikation der Index h die den verschiedenen eigenen Teilern des Ausdrucks $p^d - 1$ zukommenden Werte durchläuft; und endlich werden insgesamt die (mod. p) inkongruenten Zahlen ω des Bereichs G_α, für welche nicht $\omega \equiv 0$ (mod. p) ist, die Wurzeln der Kongruenz

$$\prod_d \prod_h \prod_i P_d^{(i)}(x) \equiv 0 \text{ (mod. } p)$$

sein, in welcher die dritte Multiplikation auf sämtliche Teiler d von n zu erstrecken ist; ihr genügt auch die Zahl $\omega \equiv 0$ (mod. p), wenn sie noch mit x multipliziert gedacht wird. Mithin erhält man, da dieselben Zahlen auch die Wurzeln der Kongruenz

$$x^{p^n} - x \equiv 0 \text{ (mod. } p)$$

im Bereiche G_α sind, die identische Beziehung

$$x^{p^n} - x \equiv x \cdot \prod_d \prod_h \prod_i P_d^{(i)}(x) \text{ (mod. } p),$$

d. h. eine Zerlegung der Funktion $x^{p^n} - x$ in Primfunktionen, welche mit der in (56) ausgesprochenen Zerlegung übereinstimmen muß. So wird die Bedeutung der dort auftretenden Primfunktionen $P_d^{(i)}(x)$ oder die Verteilung aller inkongruenten Zahlen des Bereiches G_α auf sie in das hellste Licht gesetzt: jede der mit $P_d^{(i)}(x)$ bezeichneten und von x verschiedenen Primfunktionen d^{ten} Grades hat d der zum Exponenten d passenden Zahlen ω zu Wurzeln, und zwar

bilden diese immer je eine Unterabteilung der Klassen, in welche die zu d passenden Zahlen nach dem Exponenten, zu dem sie gehören, zerfallen.

8. Zum Schluß dieser Betrachtungen fassen wir noch den besonderen Modulus

$$\{p,\ x^p - x\} \tag{78}$$

ins Auge. Ist $F(x)$ irgend eine ganze, ganzzahlige Funktion, so kann man setzen

$$F(x) = (x^p - x) \cdot \psi(x) + \varrho(x),$$

wo auch $\psi(x)$, $\varrho(x)$ solche Funktionen, die letztere vom $p-1^{\text{ten}}$ Grade bedeuten. Soll nun für jeden ganzzahligen Wert von x die Funktion $F(x)$ teilbar sein durch p, so ist dieser Gleichung zufolge und da nach dem Fermatschen Satze $x^p - x$ für jeden solchen Wert durch p aufgeht, dafür notwendig und hinreichend, daß auch $\varrho(x)$, welches die Form hat

$$\varrho(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1},$$

für jeden solchen Wert von x durch p teilbar ist, woraus dann folgt, daß die Kongruenz

$$\varrho(x) \equiv 0 \pmod{p}$$

identisch bestehe, d. h., daß $\varrho(x) = p \cdot \varphi(x)$ sei. Man erhält also den Satz:

Damit eine ganze, ganzzahlige Funktion $F(x)$ für jeden ganzzahligen Wert von x durch p teilbar sei, ist notwendig und hinreichend, daß sie von der Form

$$F(x) = p\varphi(x) + (x^p - x)\psi(x), \tag{79}$$

d. h. im Modulus (78) enthalten sei.

Dieser Satz läßt sich folgendermaßen verallgemeinern: Damit eine ganze, ganzzahlige Funktion $F(x, y, z, \cdots)$ der Unbestimmten $x, y, z, \cdots$ für alle ganzzahligen Werte der letzteren durch p teilbar sei, ist notwendig und hinreichend, daß sie von der Form

$$F(x,y,z,\cdots) = p \cdot F + (x^p - x) \cdot \Phi + (y^p - y) \cdot \Psi + (z^p - z) \cdot X + \cdots \tag{80}$$

und in dieser $F, \Phi, \Psi, X, \cdots$ ganze, ganzzahlige Funktionen von $x, y, z, \cdots$ seien, oder, was dasselbe sagt, daß sie in dem Modulus

$$\{p,\ x^p - x,\ y^p - y,\ z^p - z,\ \cdots\} \tag{81}$$

enthalten sei. Faßt man nämlich, um dies zu beweisen, $F(x, y, z, \cdots)$ als eine Funktion von x allein auf, so ist es eine ganze Funktion von x mit Koeffizienten, die ihrerseits ganze, ganzzahlige Funktionen von $y, z, \cdots$ sind, und man kann setzen:

$$(82) \quad F(x, y, z, \cdots) = (x^p - x) \cdot \Phi(x, y, z, \cdots) + P(x, y, z, \cdots),$$

wo $\Phi(x, y, z, \cdots)$, $P(x, y, z, \cdots)$ ebensolche Funktionen von x sind, die letztere vom Grade $p - 1$; diese hat somit die Gestalt

$$(83) \quad P(x, y, z, \cdots) = P_0 + P_1 \cdot x + P_2 \cdot x^2 + \cdots + P_{p-1} \cdot x^{p-1},$$

worin die P_i ganze, ganzzahlige Funktionen von $y, z, \cdots$ allein bedeuten. Soll nun für alle ganzzahligen $x, y, z, \cdots$, d. h. für ein beliebig gewähltes ganzzahliges System $y, z, \cdots$ und jede ganze Zahl x die Funktion $F(x, y, z, \cdots)$ durch p teilbar werden, so ist nach (82) notwendig wie offenbar auch hinreichend, daß auch die Funktion $P(x, y, z, \cdots)$, wenn man darin für $y, z, \cdots$ dies Zahlensystem gesetzt denkt, für jeden ganzzahligen Wert von x durch p aufgehe, daß mithin die diesem Zahlensystem $y, z, \cdots$ entsprechend bestimmte ganzzahlige Kongruenz

$$P_0 + P_1 \cdot x + P_2 \cdot x^2 + \cdots + P_{p-1} \cdot x^{p-1} \equiv 0 \pmod{p}$$

die p Wurzeln $x = 0, 1, 2, \cdots, p - 1$ zulasse, also identisch erfüllt sei. Daher findet sich als notwendige und hinreichende Bedingung, daß jede der ganzen, ganzzahligen Funktionen P_i von $y, z, \cdots$ für jedes beliebig gewählte ganzzahlige Wertsystem dieser Unbestimmten, deren Anzahl um 1 geringer ist, als die der ursprünglichen Unbestimmten $x, y, z, \cdots$, durch p teilbar sei. Setzen wir also voraus, der zu beweisende Satz stehe schon fest für die geringere Anzahl von Unbestimmten, so ergibt sich für die Koeffizienten P_i die notwendige und hinreichende Form

$$P_i = p \cdot F_i + (y^p - y) \cdot \Psi_i + (z^p - z) \cdot X_i + \cdots,$$
$$(\text{für } i = 0, 1, 2, \cdots, p-1)$$

worin die $F_i, \Psi_i, X_i, \cdots$ ganze, ganzzahlige Funktionen der $y, z, \cdots$ bezeichnen. Daraus ergibt sich $P(x, y, z, \cdots)$ wegen (83) von der folgenden Form:

$$P(x, y, z, \cdots) = p \cdot F + (y^p - y) \cdot \Psi + (z^p - z) \cdot X + \cdots,$$

wo nun F, Ψ, X, $\cdots$ ganze, ganzzahlige Funktionen der sämtlichen Unbestimmten $x, y, z, \cdots$ sein werden, und somit wegen (82) endlich auch für $F(x, y, z, \cdots)$ die in der Gleichung (80) behauptete notwendige Gestalt, die ersichtlich aber in Anbetracht des Fermatschen Satzes auch hinreichend ist. Da nun für Funktionen $F(x)$ einer Unbestimmten der Satz durch den voraufgeschickten besonderen Fall schon festgestellt ist, so ist hiermit seine Allgemeingültigkeit erwiesen. — Wir werden von diesem hier nach Hensel (Journ. für reine und angewandte Mathematik, 113 S. 144) bewiesenen Satze später mehrfachen Gebrauch zu machen haben.

Viertes Kapitel.

Die ganzen algebraischen Zahlen.

1. Nach den in den vorigen Kapiteln angestellten vorbereitenden Untersuchungen wenden wir uns nunmehr zum eigentlichen Gegenstande dieses Werks, der Theorie der ganzen algebraischen Zahlen.

In Nr. 1 des ersten Kapitels sind diese Zahlen als die Wurzeln der Gleichungen beliebigen Grades

$$(1) \qquad x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n = 0$$

mit ganzzahligen Koeffizienten definiert worden. Wie nun bei jeder gewöhnlichen ganzen Zahl die nächstliegende Frage ist, welche Teiler sie hat, so tritt auch hier zuerst die Frage nach den Teilern einer gegebenen ganzen algebraischen Zahl α an uns heran. Man nennt aber α teilbar durch eine andere Zahl β dieser Art oder ein Vielfaches von β, wenn der Quotient $\frac{\alpha}{\beta}$ wieder eine ganze algebraische Zahl oder wenn α dem Produkte $\beta\gamma$ aus β in eine ebenfalls ganze algebraische Zahl γ gleich ist. Hieraus leuchten sofort die beiden einfachen Sätze ein:

1) Sind α', α'' zwei durch die ganze Zahl β teilbare algebraische ganze Zahlen, so sind auch ihre

Summe $\alpha' + \alpha''$ und ihre Differenz $\alpha' - \alpha''$ zwei solche Zahlen; denn aus

$$\alpha' = \beta\gamma', \quad \alpha'' = \beta\gamma'',$$

wo γ', γ'' ganze algebraische Zahlen bedeuten, folgen die Gleichungen

$$\alpha' + \alpha'' = \beta(\gamma' + \gamma''), \quad \alpha' - \alpha'' = \beta(\gamma' - \gamma''),$$

wo auch (Kap. 1, Nr. 2, Zusatz) $\gamma' \pm \gamma''$ wieder ganze algebraische Zahlen sind. Man kann diese Tatsache auch dahin aussprechen, daß man sagt: die sämtlichen Vielfachen einer ganzen Zahl bilden einen Zahlenmodulus.

2) Ist eine ganze Zahl α ein Vielfaches einer ganzen Zahl β und diese selbst ein Vielfaches von der ganzen Zahl γ, so ist auch α ein Vielfaches von γ; denn aus $\alpha = \beta\delta$, $\beta = \gamma\varepsilon$ folgt $\alpha = \gamma \cdot \delta\varepsilon$, wo das Produkt $\delta\varepsilon$ der beiden ganzen Zahlen δ, ε (s. dieselbe Stelle) wieder eine solche ist.

Eine ganze algebraische Zahl ε, durch welche jede solche Zahl teilbar ist, werde eine *Einheit* genannt. Solche Zahlen gibt es, denn z. B. sind ± 1 zwei dergleichen. Eine Einheit ε muß der Definition zufolge auch ein Teiler von 1 sein, also muß $1 = \varepsilon\varepsilon'$ gesetzt werden können, wo auch ε' eine ganze Zahl ist; und umgekehrt ist, da $\alpha = 1 \cdot \alpha$ gesetzt werden kann, nach dem zweiten der voraufgehenden Sätze jeder Teiler von 1 auch Teiler jeder beliebigen ganzen Zahl α, mithin eine Einheit. Daher ist auch der reziproke Wert einer Einheit

$$\varepsilon' = \frac{1}{\varepsilon}$$

wieder eine Einheit. Da nun auch das Produkt zweier Einheiten $\varepsilon, \varepsilon_1$ wieder eine Einheit ist, indem aus Gleichungen von der Form

$$1 = \varepsilon\varepsilon', \quad 1 = \varepsilon_1\varepsilon_1'$$

auch

$$1 = \varepsilon\varepsilon_1 \cdot \varepsilon'\varepsilon_1'$$

hervorgeht, wo $\varepsilon'\varepsilon_1'$ mit $\varepsilon', \varepsilon_1'$ zugleich eine ganze Zahl ist, so folgt, daß auch der Quotient

$$\frac{\varepsilon_1}{\varepsilon} = \varepsilon_1 \cdot \frac{1}{\varepsilon} = \varepsilon_1 \cdot \varepsilon'$$

zweier Einheiten wieder eine Einheit ist. Desgleichen ist

$$\eta = \varepsilon^{\pm \frac{s}{r}}$$

mit ε zugleich für alle positiven ganzzahligen r, s eine Einheit; in der Tat muß nach den voraufgehenden Bemerkungen, da $\varepsilon^{\frac{1}{r}} = \sqrt[r]{\varepsilon}$ als eine nach Kap. 1, Nr. 3 ganze Zahl, deren r^{te} Potenz gleich ε, d. i. ein Teiler von 1 ist, selbst in der Einheit aufgeht, auch deren s^{te} Potenz sowie ihr reziproker Wert eine Einheit sein. Allgemeiner noch ist jede algebraische Zahl, die einer ganzzahligen Gleichung (1) Genüge leistet mit dem letzten Koeffizienten 1, eine Einheit, denn dieser Koeffizient ist (nach Kap. 1, Nr. 1) das Produkt aller Wurzeln jener Gleichung also teilbar durch jene Zahl. Sonach ist die Menge aller algebraischen Einheiten unendlich.

Ist der Quotient zweier ganzen Zahlen α, β eine Einheit ε, also $\alpha = \beta\varepsilon$, so heißen α, β einander assoziiert. Diese Beziehung ist gegenseitig, denn als Einheit genügt ε einer Gleichung $1 = \varepsilon\varepsilon'$, worin auch ε' eine Einheit ist, und vermittels dieser Gleichung nimmt die Beziehung

$$\alpha = \beta\varepsilon \tag{2}$$

die Gestalt an

$$\beta = \alpha\varepsilon'.$$

Auch sieht man unmittelbar ein, daß zwei Zahlen α_1, α_2, welche derselben dritten Zahl β assoziiert sind, es auch einander sein müssen; denn aus den Gleichungen

$$\alpha_1 = \beta\varepsilon_1, \quad \alpha_2 = \beta\varepsilon_2,$$

worin $\varepsilon_1, \varepsilon_2$ Einheiten sind, folgt sogleich

$$\alpha_1 = \alpha_2 \cdot \frac{\varepsilon_1}{\varepsilon_2},$$

wo der Quotient $\frac{\varepsilon_1}{\varepsilon_2}$ wieder eine Einheit ist. Man kann daher sämtliche ganze algebraische Zahlen in Gruppen verteilen, indem man stets diejenigen zusammenfaßt, welche einander assoziiert sind, und jede ganze Zahl findet sich alsdann in einer und nur einer dieser Gruppen vor. Hieraus leuchtet ein, daß in Fragen der Teilbarkeit zwei Zahlen derselben Gruppe sich durchaus gleich verhalten und

einander vertreten können: wenn nämlich α teilbar ist durch β, so wird auch jede zu α assoziierte Zahl durch jede zu β assoziierte Zahl teilbar sein, da aus einer Gleichung

$$\alpha = \beta\gamma$$

sofort

$$\alpha\varepsilon = \beta\varepsilon_1 \cdot \frac{\gamma\varepsilon}{\varepsilon_1}$$

und hier $\frac{\gamma\varepsilon}{\varepsilon_1}$ sich als eine ganze Zahl ergibt, wenn ε, ε_1 Einheiten bedeuten.

Die bisherigen Ergebnisse stimmen im wesentlichen vollständig mit den Sätzen überein, welche in analoger Weise für die Teilbarkeit der rationalen ganzen Zahlen, für die rationalen Einheiten ± 1, und für die Verteilung jener Zahlen in positive und negative Zahlen bestehen. Durchaus unterscheiden sich dagegen die ganzen algebraischen Zahlen von den ganzen rationalen, wenn man nach ihren einfachen oder unzerlegbaren oder Primfaktoren fragt: während die letzteren bekanntlich als Produkt einer endlichen Anzahl solcher unzerlegbaren Faktoren dargestellt werden können, herrscht im Gebiete aller ganzen *algebraischen* Zahlen *eine unbegrenzte Zerlegbarkeit.* In der Tat kann man eine gegebene ganze algebraische Zahl α in eine beliebig vorgeschriebene Anzahl r von Faktoren aus jenem Gebiete zerlegen einfach dadurch, daß man $\alpha = \left(\alpha^{\frac{1}{r}}\right)^r$ setzt und bemerkt daß die Zahl $\alpha^{\frac{1}{r}}$ als Wurzel der Gleichung $x^r = \alpha$ (nach Kap. 1, Nr. 3) eine ganze algebraische Zahl ist.

Nun ward man, als man zur Verallgemeinerung zahlentheoretischer Untersuchungen das Gebiet der rationalen ganzen Zahlen überschritt, nicht sogleich in das Gebiet aller ganzen algebraischen Zahlen überhaupt geführt, sondern beschränkte sich auf gewisse Arten derselben. Gauß, dem zuerst jener geniale Gedanke kam, als er, bemüht die Theorie der biquadratischen Reste auf ähnliche Gesetze zurückzuführen, wie sie diejenige der quadratischen Reste beherrschen, auf sonst unüberwindliche Schwierigkeiten stieß, bediente sich der sogenannten komplexen ganzen Zahlen von der Form $a + bi$,

worin i eine Wurzel der Gleichung $x^2 = -1$ und a, b ganze rationale Zahlen sind; für Zahlen dieser Art bestehen, wie er fand, genau die gleichen Teilbarkeitssätze, insbesondere die gleiche eindeutige Zerlegbarkeit in eine endliche Anzahl von Primfaktoren, wie in der Theorie der rationalen ganzen Zahlen. Wie wir uns überzeugen werden, sind aber jene komplexen ganzen Zahlen nichts anderes, als die ganzen algebraischen Zahlen des endlichen Körpers $K(i; R)$, der aus der Zahl i und dem Bereiche R aller rationalen Zahlen erzeugt wird. Dies legt daher den Gedanken nahe, sich bei der Untersuchung der Teilbarkeitsgesetze algebraischer Zahlen nur auf die Zahlen eines bestimmten endlichen Körpers zu beschränken; und solche Beschränkung wird in der Tat uns zu einem der bewundernswertesten allgemeinen Ergebnisse arithmetischer Spekulation, nämlich zu der Erkenntnis führen, daß für die Zahlen eines *jeden* Körpers dieser Art — freilich nur bei Einführung eines neuen außerordentlich fruchtbaren Begriffs — wieder völlig analoge Teilbarkeitsgesetze bestehen, wie in der gewöhnlichen Zahlentheorie. Diesen Nachweis zu führen, bildet die Hauptaufgabe der nächstfolgenden Abschnitte.

2. Die Zahlen ζ eines endlichen Körpers $K(\mathsf{A}; \mathfrak{R})$ n^{ten} Grades sind nach Kap. 1, Nr. 8 in $\mathfrak{R}$ algebraische Zahlen, indem sie einer Gleichung n^{ten} Grades

$$(3) \qquad \zeta^n + R_1 \zeta^{n-1} + R_2 \zeta^{n-2} + \cdots + R_n = 0$$

mit in $\mathfrak{R}$ enthaltenen Koeffizienten genügen. Hier gilt nun zunächst der einfache Satz, daß jede solche in $\mathfrak{R}$ algebraische Zahl des Körpers durch Multiplikation mit einer Zahl des Integritätsbereiches von $\mathfrak{R}$ zu einer *ganzen* in $\mathfrak{R}$ algebraischen Zahl gemacht werden kann. Sind nämlich nicht sämtliche Koeffizienten in (3) Zahlen dieses Integritätsbereiches, d. h. ist ζ nicht schon von vornherein eine in $\mathfrak{R}$ ganze Zahl, so wird man setzen dürfen

$$R_i = \frac{P_i}{P} \qquad \text{(für } i = 1, 2, \cdots, n\text{)},$$

wo die P_i sowie der gemeinsame Nenner P dem Integritäts-

bereiche angehören. Setzt man dann $\zeta' = P \cdot \zeta$, so leistet ζ' der aus (3) durch Multiplikation mit P^n hervorgehenden Gleichung

$$(4) \qquad \zeta'^n + P_1 \zeta'^{n-1} + P P_2 \zeta'^{n-2} + \cdots + P^{n-1} P_n = 0$$

Genüge, deren Koeffizienten dem Integritätsbereiche angehörig sind, und ist also eine in $\mathfrak{R}$ ganze algebraische Zahl. — Insbesondere gilt dies auch von der den Körper $\mathfrak{K} = K(\mathsf{A}; \mathfrak{R})$ erzeugenden Zahl A, für welche die Gleichung (3), der sie genügt, irreduktibel ist; da diese durch Multiplikation mit P^n nicht reduktibel werden kann, so wird also die aus A hervorgehende ganze Zahl A′ ebensowohl wie A selbst als eine erzeugende Zahl des Körpers gewählt werden können, und somit ergibt sich weiter: Jeder endliche Körper enthält eine in seinem Rationalitätsbereiche *ganze* algebraische Zahl, durch welche er erzeugt werden kann.

Ist der Rationalitätsbereich $\mathfrak{R}$ der Bereich R der rationalen Zahlen, so besteht der Satz: Jede ganze algebraische Zahl des Bereichs R gehört zu dessen Integritätsbereiche, d. h., wenn eine ganze *algebraische* Zahl *rational* ist, so ist sie sogar eine *ganze* rationale Zahl. In der Tat, wäre ζ eine Wurzel der ganzzahligen Gleichung

$$(5) \qquad \zeta^n + a_1 \zeta^{n-1} + a_2 \zeta^{n-2} + \cdots + a_n = 0$$

und wäre zugleich $\zeta = \frac{r}{s}$, wo r, s ganze Zahlen bedeuten, die ohne gemeinsamen Teiler vorausgesetzt werden können, so erhielte man aus jener Gleichung die Beziehung

$$(6) \qquad r^n = -s(a_1 r^{n-1} + a_2 s r^{n-2} + \cdots + a_n s^{n-1}),$$

welche doch unmöglich ist, da die rechte Seite ein Vielfaches von s, die linke aber relativ prim zu s ist.

Dieser Satz verstattet die Ausdehnung auf den Fall, daß der Rationalitätsbereich $\mathfrak{R}$ der Bereich aller rationalen Funktionen einer Anzahl von Unbestimmten $x_1, x_2, \cdots, x_m$ mit ganzzahligen Koeffizienten ist. Jede in diesem Bereiche ganze algebraische Größe nämlich, welche dem *Rationalitäts*bereiche angehört, ist sogar eine Größe seines *Integritäts*bereiches. Um dies für den Fall einer einzigen Unbestimmten x darzutun, genügen die Sätze des vorigen

Kapitels. Sei nämlich ζ eine Größe, welche der Gleichung (3) genügt, während deren Koeffizienten ganze, ganzzahlige Funktionen von x sind. Ist sie dann selbst eine rationale Funktion von x, so daß man, unter R, S ganze ganzzahlige Funktionen von x verstehend, $\zeta = \frac{R}{S}$ setzen darf, so ergibt sich die mit (6) analoge Gleichung

$$(7) \qquad R^n = -S(R_1 R^{n-1} + R_2 S R^{n-2} + \cdots + R_n S^{n-1}),$$

d. h. R^n müßte teilbar sein durch S. Da man aber ζ unter einfachster Form, d. i. R, S von jedem gemeinsamen rationalen Teiler befreit oder im Sinne von Kap. 3, Nr. 1 als relativ prim voraussetzen darf, so wird dann auch R^n prim gegen S, also nicht durch S teilbar sein, wie es die Gleichung (7) verlangt, es sei denn, daß S von x unabhängig ist. Man schließt leicht hieraus (vgl. Kap. 6, Nr. 3 die Sätze über den „Teiler" einer ganzen, ganzzahligen Funktion), daß $S = 1$, also ζ eine ganze, ganzzahlige Funktion von x sein muß, wie behauptet. — Für ganze Funktionen mehrerer Unbestimmten finden sich aber — worauf wir für unsere Zwecke nicht näher einzugehen brauchen — ganz ähnliche Teilbarkeitssätze, wie sie für Funktionen einer Unbestimmten in Kap. 3, Nr. 1 gegeben worden sind, und auf Grund derselben dann auch durch analoge Schlußweise der oben ausgesprochene allgemeinere Satz.

Ist dagegen der Rationalitätsbereich ein beliebiger Körper $K(\mathsf{A}; \mathfrak{R})$, so werden im allgemeinen die ganzen algebraischen Zahlen dieses Bereichs oder Körpers nicht auch immer Zahlen seines Integritätsbereichs, nämlich nicht immer als ganze, ganzzahlige Funktionen von A und den Elementen $\mathfrak{R}'$, $\mathfrak{R}''$, $\cdots$ des Bereichs $\mathfrak{R}$ darstellbar sein, selbst dann nicht, wenn als die erzeugende Zahl A selbst eine ganze algebraische Zahl gewählt wird. Einen einfachen Beleg für diese Wahrheit gibt der Körper $K(\mathsf{A}; R)$, dessen erzeugende Zahl A gleich $\sqrt{-3}$ ist; die diesem Körper oder Rationalitätsbereiche $(1, \sqrt{-3})$ angehörige kubische Einheitswurzel $\frac{-1+\sqrt{-3}}{2}$ ist ersichtlich nicht zugleich auch eine Zahl seines Integritätsbereiches, gleichwohl aber eine ganze

algebraische Zahl, weil sie der ganzzahligen Gleichung

$$x^2 + x + 1 = 0$$

Genüge leistet. **Beschränkt** man sich jedoch, wie wir fortan es tun dürfen und wollen, auf die Voraussetzung, daß der Rationalitätsbereich des endlichen Körpers der Bereich aller rationalen Zahlen ist, also auf die Betrachtung endlicher Körper von der Art $K(\mathsf{A};\, R)$, so läßt sich für die ganzen algebraischen Zahlen eines solchen Körpers eine andere allgemeine Darstellungsform nachweisen, die für all' unsere weiteren Betrachtungen die Grundlage ausmachen wird.

3. Sei also $K(\mathsf{A};\, R)$ ein endlicher Körper $\mathfrak{K}$ n^{ten} Grades mit dem Rationalitätsbereiche R aller rationalen Zahlen; seine erzeugende Zahl A darf nach voriger Nummer als eine ganze algebraische Zahl, also als Wurzel einer irreduktibeln Gleichung

$$(8) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

n^{ten} Grades mit ganzzahligen Koeffizienten vorausgesetzt werden. Die Gesamtheit aller ganzen algebraischen Zahlen dieses Körpers werde fortan mit $\mathfrak{g}$ bezeichnet. Nach den Eigenschaften ganzer algebraischer Zahlen einerseits und der Definition eines Körpers andererseits sieht man sogleich, daß die Zahlen in $\mathfrak{g}$ durch Additionen, Subtraktionen und Multiplikationen sich reproduzieren, da Summe, Differenz und Produkt von zwei solchen Zahlen wieder sowohl ganze algebraische Zahlen als auch Zahlen des Körpers sind. Ebenso gehören alle rationalen ganzen Zahlen der Gesamtheit $\mathfrak{g}$ an, sodaß man für diese Gesamtheit, welche einen Modulus bildet, die Beziehungen

$$(9) \qquad \mathfrak{z} \succ \mathfrak{g}, \quad \mathfrak{g}\mathfrak{g} \succ \mathfrak{g}$$

aufstellen darf, welche (Kap. 2, Nr. 2) dieselbe als eine Ordnung ganzer Zahlen des Körpers charakterisieren; die zweite derselben darf genauer durch die Gleichheit

$$(10) \qquad \mathfrak{g}\mathfrak{g} = \mathfrak{g}$$

ausgedrückt werden. Es mag aber sogleich hinzugefügt wer-

den, daß $\mathfrak{g}$ nicht immer die einzige Ordnung ganzer Zahlen ist, welche im Körper vorhanden ist.

Nach Kap. 1, Nr. 8 ist jede in dem hier betrachteten Körper befindliche Zahl ζ Wurzel einer Gleichung n^{ten} Grades

$$\varphi(x) = x^n + r_1 x^{n-1} + r_2 x^{n-2} + \cdots + r_n = 0 \tag{11}$$

mit rationalen Koeffizienten. Daraus allein nun, daß man ζ als ganze algebraische Zahl voraussetzt, würde noch nicht folgen, daß die Koeffizienten der für sie charakteristischen Gleichung (11) ganzzahlig sind, z. B. ist (Dedekind) $\sqrt{2}$ eine, der Gleichung

$$x^3 + \tfrac{1}{2} x^2 - 2x - 1 = 0, \tag{12}$$

deren Koeffizienten nicht sämtlich ganzzahlig sind, genügende und doch zugleich als Wurzel der Gleichung $x^2 = 2$ eine ganze algebraische Zahl. Gleichwohl gilt die Folgerung für ganze Zahlen des vorliegenden Körpers. In der Tat ist $\varphi(x)$ nach Kap. 1, Nr. 13 eine Potenz einer anderen ganzen Funktion $\psi(x)$ mit gleichfalls rationalen Koeffizienten, welche irreduktibel ist; da nun ζ, wenn es eine ganze algebraische Zahl ist, auch Wurzel einer gewissen ganzzahligen Funktion ist, welche doch, wie schon einmal bemerkt worden, nur ganzzahlige Teiler haben kann, so muß die Funktion $\psi(x)$, da sie notwendig ein Teiler derselben ist, eine ganzzahlige sein; dann ist aber auch ihre Potenz, nämlich die Funktion $\varphi(x)$ eine solche mit ganzzahligen Koeffizienten. Hiernach ist jede Zahl ζ in $\mathfrak{g}$ Wurzel einer Gleichung (11) mit ganzzahligen Koeffizienten.

Da aber die mit ζ konjugierten Zahlen $\zeta^{(1)}, \zeta^{(2)}, \cdots, \zeta^{(n-1)}$ derselben Gleichung genügen, so sind auch sie ganze algebraische Zahlen, die freilich nicht immer sämtlich ebenfalls dem Körper $\mathfrak{K} = K(\mathsf{A};\, R)$ anzugehören brauchen. Hieraus folgt dann weiter, daß auch die Spur $S(\zeta)$, die Norm $N(\zeta)$, sowie die Diskriminante

$$\Delta(\zeta) = \Delta(1, \zeta, \zeta^2, \cdots, \zeta^{n-1}) \tag{13}$$

jeder Zahl ζ in $\mathfrak{g}$, weil nur aus ganzen algebraischen Zahlen durch Additionen, Subtraktionen und Multi-

plikationen gebildet, eine ganze *algebraische* Zahl, und, da sie nach Kap. 1 zugleich eine Zahl des Rationalitätsbereichs R ist, sogar eine ganze *rationale* Zahl, mithin sicher in $\mathfrak{g}$ enthalten sein muß.

Sind nun θ, η zwei bestimmte Zahlen in $\mathfrak{g}$ und ist θ teilbar durch η, so daß die Gleichheit $\theta = \eta \cdot \zeta$ erfüllt und ζ ebenfalls eine ganze Zahl ist, so muß auch ζ in $\mathfrak{g}$ enthalten sein, denn $\zeta = \frac{\theta}{\eta}$ ist eine ganze, aber auch dem Körper $\mathfrak{K}$ zugehörige Zahl. Aus der Beziehung zwischen den Zahlen θ, η, ζ folgt aber zudem nach Kap. 1 (45) auch die entsprechende Beziehung

$$N(\theta) = N(\eta) \cdot N(\zeta) \tag{14}$$

zwischen ihren Normen. Da ferner

$$N(\theta) = \theta \cdot \theta^{(1)} \cdot \theta^{(2)} \ldots \theta^{(n-1)} \tag{15}$$

ist, wenn $\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n-1)}$ die zu θ konjugierten also ganze algebraische Zahlen bedeuten, so ist $N(\theta)$ teilbar durch θ und, da mit der Zahl θ, wie bemerkt, auch ihre Norm der Gesamtheit $\mathfrak{g}$ angehört, dem eben Gesagten zufolge der Quotient

$$\theta^{(1)} \cdot \theta^{(2)} \ldots \theta^{(n-1)} \tag{16}$$

eine ebenfalls in $\mathfrak{g}$ enthaltene Zahl.

Unter einer Einheit in $\mathfrak{g}$ verstehen wir jede in $\mathfrak{g}$ enthaltene Zahl ε, durch welche alle Zahlen dieser Gesamtheit teilbar sind. Da eine solche Zahl auch die in $\mathfrak{g}$ enthaltene Zahl 1 teilen muß, ist sie stets auch in dem früheren Sinne eine Einheit, wie denn auch umgekehrt jede Einheit ε im allgemeineren Sinne, wenn sie in $\mathfrak{g}$ enthalten ist, eine Einheit in $\mathfrak{g}$ ist, da zugleich mit 1 auch jede andere Zahl in $\mathfrak{g}$ durch ε teilbar ist. Die charakteristische Eigenschaft einer Einheit ε in $\mathfrak{g}$ kann deshalb auch darin gesetzt werden, daß ε eine Zahl in $\mathfrak{g}$ sei, deren Norm

$$N(\varepsilon) = \pm 1 \tag{17}$$

ist. Denn erstens ist eine Zahl ε in $\mathfrak{g}$, welche diese Bedingung erfüllt, ein Teiler von 1 und somit auch von jeder anderen

in $\mathfrak{g}$ enthaltenen Zahl; wenn aber umgekehrt ε eine Einheit in $\mathfrak{g}$ ist, so hat man auch

$$1 = \varepsilon\varepsilon',$$

wo der Quotient $\varepsilon' = \frac{1}{\varepsilon}$ zugleich eine Einheit und in $\mathfrak{g}$ enthalten ist, und aus dieser Gleichung folgt

$$1 = N(\varepsilon) \cdot N(\varepsilon'),$$

wo beide Normen rationale ganze Zahlen sind, mithin muß $N(\varepsilon) = \pm 1$ sein. Man darf auch sagen: Eine Zahl ε ist dann und nur dann eine Einheit in $\mathfrak{g}$, wenn $\varepsilon \cdot \mathfrak{g} = \mathfrak{g}$, d. h. wenn durch Multiplikation jeder Zahl in $\mathfrak{g}$ mit ε wieder eine Zahl in $\mathfrak{g}$ und solcherweise auch jede dieser Zahlen entsteht. Ist nämlich ε eine Einheit in $\mathfrak{g}$, so folgt aus (9) für jede in $\mathfrak{g}$ enthaltene Zahl γ, daß $\varepsilon\gamma \succ \mathfrak{g}$ ist; und, setzt man $1 = \varepsilon\varepsilon'$, so gehört ε' und folglich auch $\varepsilon'\gamma$ zu $\mathfrak{g}$, und jede in $\mathfrak{g}$ enthaltene Zahl $\gamma = \varepsilon \cdot \varepsilon'\gamma$ entsteht aus einer Zahl in $\mathfrak{g}$ durch Multiplikation mit ε. Erfüllt umgekehrt eine Zahl ε jene Bedingungen, so folgt aus der ersten, daß $\varepsilon = \varepsilon \cdot 1$ zu $\mathfrak{g}$ gehört; nach der zweiten aber muß auch $1 = \varepsilon \cdot \gamma$ sein, wo γ zu $\mathfrak{g}$ gehört, und somit ist ε eine Einheit in $\mathfrak{g}$.

Nun nannten wir zwei Zahlen γ, γ' einander assoziiert, wenn $\gamma = \varepsilon\gamma'$ gesetzt werden kann, während ε eine Einheit ist. Handelt es sich ausschließlich um Zahlen in $\mathfrak{g}$, so kann eine solche Gleichung nur statthaben, wenn ε speziell eine Einheit in $\mathfrak{g}$ ist; denn dann gehört die Einheit ε als Quotient $\frac{\gamma}{\gamma'}$ zu $\mathfrak{g}$. Man ersieht hieraus, daß zur Verteilung aller Zahlen der Gesamtheit $\mathfrak{g}$ in Gruppen assoziierter Zahlen nur die Einheiten in $\mathfrak{g}$ heranzuziehen sind, auf die wir also fortan, wenn nichts anderes gesagt wird, uns völlig beschränken, und die wir deshalb, ohne ein Mißverständnis befürchten zu müssen, kurz als Einheiten (ohne den Zusatz: in $\mathfrak{g}$) bezeichnen dürfen.

Ist eine in $\mathfrak{g}$ enthaltene Zahl γ keine Einheit, so hat sie mindestens einen Teiler in $\mathfrak{g}$, der ebenfalls keine Einheit ist, da man $\gamma = \gamma \cdot 1$ setzen darf. Ist aber in $\mathfrak{g}$ ein Teiler β von γ vorhanden, der weder eine Einheit noch mit γ gleich oder assoziiert ist, sodaß $\gamma = \beta\delta$ gesetzt werden kann, wo auch δ

weder eine Einheit noch auch mit γ assoziiert ist, so darf γ in $\mathfrak{g}$ zerlegbar heißen und es folgt die Gleichung

$$N(\gamma) = N(\beta) \cdot N(\delta),$$

während $N(\beta)$, $N(\delta)$ von ± 1 verschieden und rationale ganze Zahlen sind. Demnach muß numerisch

$$N(\beta) < N(\gamma)$$

sein. Wäre also auch β noch in $\mathfrak{g}$ zerlegbar, d. h. $\beta = \beta'\delta'$, wo wieder β', δ' Zahlen in $\mathfrak{g}$ aber weder eine Einheit noch mit β assoziiert sind, so wäre $\gamma = \beta' \cdot \delta\delta'$, wo numerisch

$$N(\beta') < N(\beta)$$

ist, usw. Die so entstehende Reihe ganzer Zahlen $N(\beta)$, $N(\beta')$, $N(\beta'')$, $\cdots$ kann als eine absolut abnehmende nur eine endliche sein, und somit ergibt sich zuletzt ein Teiler $\theta = \beta^{(k)}$ von γ, welcher nicht mehr zerlegbar ist. Setzt man dann wieder $\gamma = \theta \cdot \gamma'$ also $N(\gamma) = N(\theta) \cdot N(\gamma')$, so ist $N(\gamma') < N(\gamma)$; aus gleichem Grunde aber darf man $\gamma' = \theta' \cdot \gamma''$ setzen, wo θ' ein unzerlegbarer Teiler von γ' ist, und man findet $N(\gamma'') < N(\gamma')$, usw., ein Fortgang, der wieder nur ein endlicher sein kann und schließlich also die Zerlegung der Zahl γ in eine endliche Anzahl von in $\mathfrak{g}$ enthaltenen und unzerlegbaren Teilern:

$$\gamma = \theta \cdot \theta' \cdot \theta'' \cdots \theta^{(s)}, \tag{18}$$

d. i. die beschränkte Zerlegbarkeit der ganzen algebraischen Zahlen des Körpers $\mathfrak{K} = K(\mathsf{A}; R)$ ergibt. Mit diesem leicht gefundenen Ergebnisse ist man jedoch noch weit entfernt davon, die am Schlusse von Nr. 1 ausgesprochene Behauptung begründet zu haben. Denn diese würde wesentlich noch die Aussage erfordern, daß die Zerlegung (18) einer Zahl γ in $\mathfrak{g}$, die durch die bisherige Betrachtung nur als überhaupt möglich erwiesen ist, auch nur auf eine einzige, bestimmte Weise möglich, eine nur eindeutige Zerlegung sei. Es gibt aber im Gegenteil, wie wir uns bald überzeugen werden, Körper — und diese Körper bilden keine Ausnahme, sondern die Regel — für deren ganze Zahlen eine eindeutige Zerlegung nicht vorhanden ist.

4. In der weiteren Verfolgung unseres Zieles treten uns

vor allem die beiden Elementarsätze in Nr. 1 entgegen, welche offenbar auch bei der Beschränkung auf Zahlen der Gesamtheit $\mathfrak{g}$ in Gültigkeit bleiben. Dem ersten derselben zufolge bilden alle Zahlen in $\mathfrak{g}$, welche durch eine bestimmte θ von ihnen teilbar sind, nämlich alle Zahlen von der Form $\theta \cdot \gamma$, unter γ sämtliche Zahlen in $\mathfrak{g}$ verstanden, einen Modulus von Zahlen, den wir durch das Zeichen

$$\{\theta\} \tag{19}$$

ausdrücken und wieder nur als eine andere Deutung des Teilers θ selbst ansehen können. Allgemeiner bezeichnet hier der Modulus

$$\{\theta, \theta', \theta'', \cdots, \theta^{(m-1)}\}, \tag{20}$$

wo unter $\theta, \theta', \theta'', \cdots, \theta^{(m-1)}$ irgend welche Zahlen in $\mathfrak{g}$ gedacht werden, die Gesamtheit aller offenbar in $\mathfrak{g}$ enthaltenen Zahlen von der Form

$$f = \theta\gamma + \theta'\gamma' + \theta''\gamma'' + \cdots + \theta^{(m-1)}\gamma^{(m-1)}, \tag{21}$$

wenn darin für $\gamma, \gamma', \gamma'', \cdots, \gamma^{(m-1)}$ die sämtlichen Zahlen der Gesamtheit $\mathfrak{g}$ gesetzt werden. Einem solchen Modulus kommt die charakteristische Eigenschaft zu, daß das Produkt aus jeder seiner Zahlen in irgend eine der Zahlen in $\mathfrak{g}$ wieder ihm angehört. Wir wollen nun allgemein nach *Dedekind* eine Gesamtheit von Zahlen in $\mathfrak{g}$, welche einen Modulus bildet und dieser charakteristischen Eigenschaft genießt, *ein Ideal des Körpers* $K(\mathsf{A}; R)$ nennen und allgemein mit $\mathfrak{j}$ bezeichnen.

Demnach ist der Modulus (20) ein Ideal. — Für ein solches sind die Beziehungen

$$\mathfrak{j} \succ \mathfrak{g}, \quad \mathfrak{g}\mathfrak{j} \succ \mathfrak{j} \tag{22}$$

charakteristisch. Da $\mathfrak{g}$ auch die Zahl 1, mithin $\mathfrak{g} \cdot \mathfrak{j}$ auch $1 \cdot \mathfrak{j}$ enthält, so gilt auch die Beziehung $\mathfrak{j} \succ \mathfrak{g}\mathfrak{j}$, sodaß die zweite der vorstehenden Beziehungen auch schärfer als die Gleichheit

$$\mathfrak{g}\mathfrak{j} = \mathfrak{j} \tag{22a}$$

zu fassen ist.

Aus dieser Definition des Ideals fließen zunächst zwei einfache Folgerungen:

1) Sind $\theta_1, \theta_2, \theta_3, \cdots$ irgend welche Zahlen des Ideals $\mathfrak{j}$, so ist auch, unter $\gamma_1, \gamma_2, \gamma_3, \cdots$ irgend welche Zahlen in $\mathfrak{g}$ verstanden, die Zahl

$$\theta_1\gamma_1 + \theta_2\gamma_2 + \theta_3\gamma_3 + \cdots$$

im Ideale enthalten.

2) Ist θ eine Zahl des Ideals $\mathfrak{j}$, so ist's auch ihre Norm, denn $N(\theta)$ ist gleich θ mal der nach der vorigen Nummer in $\mathfrak{g}$ enthaltenen Zahl $\theta^{(1)}\theta^{(2)} \ldots \theta^{(n-1)}$.

Nun gibt es (nach Kap. 1, Nr. 8), im endlichen Körper $K(\mathsf{A}; R)$ n^{ten} Grades n von einander unabhängige Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ von der Beschaffenheit, daß jede Zahl des Körpers in der Form

$$r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$$

dargestellt werden kann, indem man für die r_i Zahlen des Rationalitätsbereiches, hier also rationale Zahlen setzt. Die Basiszahlen $\omega_1, \omega_2, \cdots, \omega_n$ dürfen hierbei sogar als ganze Zahlen des Körpers, d. i. als Zahlen in $\mathfrak{g}$ vorausgesetzt werden; denn, sind $c_1, c_2, \ldots, c_n$ passende rationale Zahlen, durch welche multipliziert $\omega_1, \omega_2, \cdots, \omega_n$ resp. in ganze Zahlen

$$\gamma_1 = c_1\omega_1, \; \gamma_2 = c_2\omega_2, \; \cdots, \; \gamma_n = c_n\omega_n$$

des Körpers übergehen, so sind auch diese n Zahlen rational unabhängig, da eine Beziehung

$$a_1\gamma_1 + a_2\gamma_2 + \cdots + a_n\gamma_n = 0$$

mit rationalen, nicht sämtlich verschwindenden Koeffizienten die Beziehung

$$a_1c_1 \cdot \omega_1 + a_2c_2 \cdot \omega_2 + \cdots + a_nc_n \cdot \omega_n = 0$$

derselben Art nach sich ziehen würde. Demnach dürfen auch die ganzen Zahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ des Körpers als eine Basis desselben gewählt und mithin wird jede seiner Zahlen, insbesondere jede Zahl in $\mathfrak{g}$ in der Form

$$r_1\gamma_1 + r_2\gamma_2 + \cdots + r_n\gamma_n \tag{23}$$

mit rationalen Koeffizienten dargestellt werden. Wenn hier den Koeffizienten ganzzahlige Werte erteilt werden, so wird die entstehende Zahl selbstverständlich eine Zahl in $\mathfrak{g}$ sein; doch ist damit durchaus nicht gesagt, daß so auch alle

Zahlen in $\mathfrak{g}$ entstehen, oder daß nicht auch rationalen Werten der Koeffizienten solche Zahlen entsprechen; es würde sich darum handeln, diejenigen Werte der Koeffizienten auszusondern, welche die ganzen Zahlen und nur sie ergeben. Jedenfalls aber gilt die allgemeine Form (23) der Zahlen in $\mathfrak{g}$ auch für die Zahlen in $\mathfrak{j}$. Unter den letzteren gibt es daher auch solche, welche in der Form (23) mit ganzzahligen Koeffizienten darstellbar sind, denn, ist

$$\theta = r_1\gamma_1 + r_2\gamma_2 + \cdots + r_n\gamma_n$$

eine Zahl des Ideals mit rationalen Koeffizienten und allgemein $r_i = \frac{g_i}{g}$, wo g und die Zahlen g_i ganze Zahlen bedeuten, so wird

$$g\theta = g_1\gamma_1 + g_2\gamma_2 + \cdots + g_n\gamma_n \tag{23^a}$$

eine im Ideale enthaltene Zahl mit ganzzahligen Koeffizienten sein. Nun gibt es wieder unter den letzteren Zahlen des Ideals auch solche von der Form

$$\theta_s = g_1^{(s)}\gamma_1 + g_2^{(s)}\gamma_2 + \cdots + g_s^{(s)}\gamma_s,$$

wo s eine beliebige der Zahlen $1, 2, \cdots, n$ und $g_s^{(s)}$ von Null verschieden ist; in der Tat, wenn θ irgend eine von Null verschiedene, somit auch $N(\theta)$ eine Zahl des Ideals bedeutet, so ist $N(\theta)\cdot\gamma_s$ eine Zahl des Ideals von der behaupteten Form. Stellt man aber in dieser Weise n Zahlen des Ideals auf:

$$\begin{aligned}
\theta_1 &= g_1^{(1)}\cdot\gamma_1 \\
\theta_2 &= g_1^{(2)}\cdot\gamma_1 + g_2^{(2)}\cdot\gamma_2 \\
\theta_3 &= g_1^{(3)}\cdot\gamma_1 + g_2^{(3)}\cdot\gamma_2 + g_3^{(3)}\cdot\gamma_3 \\
&\cdots\cdots\cdots\cdots \\
\theta_n &= g_1^{(n)}\cdot\gamma_1 + g_2^{(n)}\cdot\gamma_2 + g_3^{(n)}\cdot\gamma_3 + \cdots + g_n^{(n)}\cdot\gamma_n,
\end{aligned} \tag{24}$$

so bilden dieselben, da die Determinante

$$g_1^{(1)}\cdot g_2^{(2)}\cdots g_n^{(n)}$$

dieser Gleichungen von Null verschieden ist, von neuem eine Basis des Körpers und folglich ist jede Zahl desselben, insbesondere auch jede Zahl θ des Ideals $\mathfrak{j}$ von der Form

$$\theta = r_1\theta_1 + r_2\theta_2 + \cdots + r_n\theta_n \tag{25}$$

mit rationalen Koeffizienten. Betrachten wir einstweilen nur diejenigen Zahlen

$$(26) \qquad \theta_0 = \varrho_1 \theta_1 + \varrho_2 \theta_2 + \cdots + \varrho_n \theta_n$$

des Ideales, deren Koeffizienten ϱ_i den Bedingungen

$$(27) \qquad 0 \gtreqless \varrho_i \gtreqless 1$$

genügen; solche Zahlen gibt es, z. B. die Zahlen $\theta_1, \theta_2, \cdots, \theta_n$. Wie wir nachher zeigen werden, ist die Anzahl aller Zahlen dieser Art im ganzen Körper eine nur endliche; dies gilt also um so mehr für die Anzahl derjenigen von ihnen, welche dem Ideale $\mathfrak{j}$ angehören. Man kann daher die letztgedachten Zahlen in n endliche Gruppen verteilen, so daß in der s^{ten} Gruppe diejenigen von ihnen liegen, welche die Gestalt

$$(28) \qquad \theta^{(s)} = \varrho_1^{(s)} \theta_1 + \varrho_2^{(s)} \theta_2 + \cdots \varrho_s^{(s)} \theta_s$$

haben, während wieder $0 \gtreqless \varrho_i^{(s)} \gtreqless 1$, insbesondere aber $\varrho_s^{(s)}$ von Null verschieden ist; da θ_s selbst eine solche Zahl ist, enthält jede der bezeichneten Gruppen mindestens eine Zahl und unter ihnen allen sei $\theta_0^{(s)}$ eine von denjenigen, bei welchen $\varrho_s^{(s)}$ den kleinsten Wert habe, welcher σ_s heiße. Denkt man sich diese, den einzelnen Gruppen entsprechenden Zahlen

$$\theta_0^{(1)},\ \theta_0^{(2)},\ \cdots,\ \theta_0^{(n-1)},\ \theta_0^{(n)}$$

mit den letzten Koeffizienten $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}, \sigma_n$ resp. gebildet, so wird man durch Subtraktion eines ganzen Vielfachen von $\theta_0^{(n)}$ von der in der Form (25) gegebenen Zahl θ des Ideals $\mathfrak{j}$ eine andere Zahl desselben erhalten, in welcher der letzte Koeffizient, wenn er nicht Null ist, positiv und kleiner als σ_n ist; aus dieser wieder durch Subtraktion eines Vielfachen von $\theta_0^{(n-1)}$ eine neue Zahl des Ideals, deren vorletzter Koeffizient Null oder positiv und kleiner als σ_{n-1} ist, während der letzte unverändert blieb, u. s. w.; kurz man darf setzen

$$(29) \qquad \theta = g_1 \theta_0^{(1)} + g_2 \theta_0^{(2)} + \cdots + g_n \theta_0^{(n)} + \theta_0,$$

worin die Koeffizienten g_i ganze rationale Zahlen, θ_0 aber eine Zahl des Ideals von der Form (26) ist, deren Koeffizienten den Bedingungen genügen

$$0 \gtreqless \varrho_i < \sigma_i,$$

was doch der Bedeutung der Koeffizienten σ_i zufolge nur sein kann, wenn allgemein $\varrho_i = 0$, also auch $\theta_0 = 0$ ist. So nimmt die Gleichung (29) die Gestalt an:

$$(30) \qquad \theta = g_1 \theta_0^{(1)} + g_2 \theta_0^{(2)} + \cdots g_n \theta_0^{(n)}$$

und lehrt als Endergebnis unserer Betrachtung, daß es im Ideale $\mathfrak{j}$ stets n unabhängige Zahlen $\theta_0^{(1)}, \theta_0^{(2)}, \cdots, \theta_0^{(n)}$ gibt von der Beschaffenheit, daß jede Zahl desselben durch sie in der Gestalt (30) mittels ganzzahliger Koeffizienten dargestellt werden kann. Aber auch umgekehrt wird dann jede Zahl dieser Gestalt eine Zahl des Ideals sein. Man erkennt hieraus den Satz:

Jedes Ideal des Körpers ist ein (im *Dedekind*schen Sinne zu nehmender) n-gliedriger Modulus

$$(31) \qquad [\theta_0^{(1)}, \theta_0^{(2)}, \cdots, \theta_0^{(n)}],$$

dessen Basis aus Zahlen in $\mathfrak{g}$ besteht.

Daß die Zahlen $\theta_0^{(1)}, \theta_0^{(2)}, \cdots, \theta_0^{(n)}$ unabhängige Zahlen sind, folgt einfach daraus, daß auch die n von einander unabhängigen Zahlen $\theta_1, \theta_2, \cdots, \theta_n$ des Körpers linear durch sie darstellbar sind; denn, ließen sich jene durch nur einen Teil von ihnen linear ausdrücken, so müßte auch zwischen diesen eine lineare Gleichung mit rationalen Koeffizienten bestehen.

Zur vollständigen Begründung dieses wichtigen Satzes fehlt noch der Nachweis, daß die Anzahl der Zahlen (26) bei Geltung der Ungleichheiten (27) nur endlich ist. Hierzu bedienen wir uns des nachstehenden Hilfssatzes:

Es gibt unter allen ganzen algebraischen Zahlen, welche Körpern n^{ten} Grades von der Art $K(\mathsf{A}; R)$ angehören, nur eine endliche Anzahl von solchen, die nebst allen ihren Konjugierten dem absoluten Betrage nach nicht größer sind, als ein gegebener Wert. In der Tat werden dann auch die nach Nr. 3 ganzzahligen Koeffizienten der Gleichung n^{ten} Grades, der eine solche Zahl genügt, da sie die einfachsten symmetrischen Funktionen aller Konjugierten sind, nach ihrem absoluten Werte nicht über einer nur durch n und den gegebenen Wert bestimmten Grenze liegen und demnach als rationale ganze Zahlen nur eine end-

liche Menge von Werten haben können, sodaß dann auch nur eine endliche Menge von Gleichungen vorhanden ist, als deren Wurzeln jene ganzen algebraischen Zahlen bestimmt sind.

Da nun, wenn $0 \overline{\overline{<}} \varrho_i \overline{\overline{<}} 1$ ist, nach der Formel (26) jedenfalls

$$\text{mod. } \theta_0 \overline{\overline{<}} \text{mod. } \theta_1 + \text{mod } \theta_2 + \cdots + \text{mod. } \theta_n$$

ist und, weil die Formel (26) bestehen bleibt, wenn statt der Zahlen $\theta_0, \theta_1, \theta_2, \cdots, \theta_n$ ihre Konjugierten gesetzt werden, eine entsprechende Ungleichheit für die absoluten Beträge der Konjugierten von θ_0 erschlossen wird, so trifft für die ganzen algebraischen Zahlen θ_0, deren Koeffizienten ϱ_i jener Ungleichheit genügen, die Annahme des Hilfssatzes zu, falls die größte der oberen Grenzen für jene absoluten Beträge als der gegebene Wert gedacht wird; damit ist aber der oben verlangte Nachweis erbracht.

Bedenkt man jetzt, daß der Modulus $\mathfrak{g}$ aller ganzen algebraischen Zahlen des Körpers $\mathfrak{K}$, da er wegen (9) auch den Bedingungen (22):

$$\mathfrak{g} \succ \mathfrak{g}, \ \mathfrak{g}\mathfrak{g} \succ \mathfrak{g}$$

genügt, selbst ein Ideal des Körpers ist, so fließt aus dem nun vollständig begründeten Idealsatze auch die in Nr. 2 verheißene allgemeine Darstellungsform der Zahlen in $\mathfrak{g}$; denn nach jenem Satze gibt es n von einander unabhängige ganze algebraische Zahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ des Körpers von der Beschaffenheit, daß die Gesamtheit der Zahlen in $\mathfrak{g}$ durch die Formel

$$\gamma = g_1\gamma_1 + g_2\gamma_2 + \cdots + g_n\gamma_n \tag{32}$$

dargestellt wird, wenn darin für die Koeffizienten g_i alle rationalen ganzen Zahlen gesetzt werden. Mit anderen Worten: diese Gesamtheit $\mathfrak{g}$ ist identisch mit dem n-gliedrigen Modulus

$$\mathfrak{g} = [\gamma_1, \gamma_2, \cdots, \gamma_n]. \tag{33}$$

Die Basis $\gamma_1, \gamma_2, \cdots, \gamma_n$ dieses Modulus soll auch eine Basis von $\mathfrak{g}$ genannt werden. (Vgl. hierzu Minkowski, Geometrie der Zahlen, § 41).

5. Hieran fügen wir zunächst als Grundlage für spätere Betrachtungen eine Reihe von Folgerungen.

Die Basis von $\mathfrak{g}$ ist keine eindeutig bestimmte, vielmehr wissen wir aus Kap. 2, Nr. 5, daß sie durch jedes System von Zahlen

(34) $$\gamma_i' = c_{1i}\gamma_1 + c_{2i}\gamma_2 + \cdots + c_{ni}\gamma_n, \quad (i = 1, 2, \cdots, n)$$

in welchen die ganzzahligen Koeffizienten c_{ik} eine der positiven oder negativen Einheit gleiche Determinante haben, und welche in $\mathfrak{g}$ enthalten sind, doch auch nur durch ein solches System ersetzt werden können.

Denken wir dagegen irgend ein System (34) von n in $\mathfrak{g}$ enthaltenen Zahlen γ_i', indem wir den ganzzahligen Koeffizienten c_{ik} nur die einzige Beschränkung auferlegen, daß ihre Determinante nicht verschwinde, so werden diese Zahlen γ_i' zwar nicht immer eine Basis von $\mathfrak{g}$, aber, weil unabhängig von einander, eine Basis des Körpers $\mathfrak{K}$ sein. Der in $\mathfrak{g}$ enthaltene Modulus

$$\mathfrak{m} = [\gamma_1', \gamma_2', \cdots, \gamma_n']$$

wird mithin ein n-gliedriger Modulus sein. Wir können derartige n-gliedrige Moduln hinfort „Moduln in $\mathfrak{g}$" nennen, dürfen jedoch dafür kürzer auch schlechthin „Modul" sagen, wo kein Mißverständnis zu befürchten ist. Jedes Ideal des Körpers, insbesondere also $\mathfrak{g}$ selbst, ist ein derartiger Modulus. Die Diskriminante

$$\Delta(\gamma_1', \gamma_2', \cdots, \gamma_n')$$

der *Basis* des Modulus möge kurz die Diskriminante $\Delta(\mathfrak{m})$ des *Modulus* heißen.

Aus den Beziehungen (34) geht (s. Kap. 1, (51)) die Gleichung hervor:

(35) $$\Delta(\gamma_1', \gamma_2', \cdots, \gamma_n') = |c_{ik}|^2 \cdot \Delta(\gamma_1, \gamma_2, \cdots, \gamma_n)$$

oder

(36) $$\Delta(\mathfrak{m}) = |c_{ik}|^2 \cdot \Delta(\mathfrak{g}).$$

Ist das System der γ_i' nur eine andere Basis von $\mathfrak{g}$, nämlich $|c_{ik}| = \pm 1$, so ergibt sich $\mathfrak{m} = \mathfrak{g}$ und $\Delta(\mathfrak{m}) = \Delta(\mathfrak{g})$, d. h. die Diskriminante von $\mathfrak{g}$ ist unabhängig von der Wahl der besonderen Basis von $\mathfrak{g}$. Da allgemein sowohl die Zahlen γ_i als die Zahlen γ_i' eine Basis des Körpers bilden, so sind die Diskriminanten $\Delta(\mathfrak{g})$, $\Delta(\mathfrak{m})$ von Null verschiedene, ganze rationale Zahlen (s. Nr. 3), mithin ist, da auch $|c_{ik}|$ eine solche

ist, die Diskriminante von $\mathfrak{g}$ gemeinsamer Teiler aller, den verschiedenen „Moduln in $\mathfrak{g}$“ entsprechenden Diskriminanten. Zu diesen Moduln zählt, da die den Körper erzeugende Zahl A als ganze algebraische Zahl vorausgesetzt ist, auch der Modulus

$$[1, \mathsf{A}, \mathsf{A}^2, \cdots, \mathsf{A}^{n-1}],$$

dessen Diskriminante nach Kap. 1, (74) durch

$$\Delta(\mathsf{A}) = (-1)^{\frac{n(n-1)}{2}} \cdot Nf'(\mathsf{A}) \tag{37}$$

ausgedrückt werden kann; also ist $\Delta(\mathfrak{g})$ auch ein Teiler dieses letztern Ausdrucks. Hiernach ist unter den Diskriminanten aller Moduln in $\mathfrak{g}$ die Diskriminante von $\mathfrak{g}$ selbst die absolut kleinste und eine eindeutig bestimmte Zahl. Sie soll, weil von fundamentalster Bedeutung für die Theorie, die Diskriminante oder die *Grundzahl* des Körpers $\mathfrak{K} = K(\mathsf{A}; R)$ genannt und durch das Zeichen D angedeutet werden:

$$\mathrm{D} = \Delta(\mathfrak{g}). \tag{38}$$

Bedeutet $2q$ die Anzahl imaginärer Wurzeln der den Körper erzeugenden Gleichung (8), so hat die Grundzahl D das Vorzeichen von $(-1)^q$. In der Tat, in der Determinante

$$\Gamma = \begin{vmatrix} \gamma_1, & \gamma_2, \cdots\cdots, & \gamma_n \\ \gamma_1^{(1)}, & \gamma_2^{(1)}, \cdots\cdots, & \gamma_n^{(1)} \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ \gamma_1^{(n-1)}, & \gamma_2^{(n-1)} \cdots, & \gamma_n^{(n-1)} \end{vmatrix}, \tag{39}$$

deren einzelne Reihen die Konjugierten zu den Zahlen der ersten Reihe sind, und deren Quadrate die Diskriminante $\Delta(\mathfrak{g})$ gleich ist, werden die Zahlen einer Reihe, die einer reellen Wurzel der Gleichung (8) entspricht, reell, die Zahlen zweier Reihen, welche zwei konjugiert imaginären Wurzeln dieser Gleichung entsprechen, selbst einander resp. konjugiert imaginär sein. Vertauscht man daher i mit $-i$ in dem Ausdrucke der Determinante (39), so werden je zwei solche Reihen sich mit einander vertauschen und, da so q Vertauschungen zweier Reihen stattfinden, Γ übergehen in $(-1)^q \Gamma$. Also geht aus dem Ausdrucke

$$\Gamma = \Gamma' + i\Gamma''$$

der folgende

$$\Gamma' - i\Gamma'' = (-1)^q \cdot (\Gamma' + i\Gamma'')$$

hervor, d. h. es ist,

wenn q gerade ist, $\Gamma'' = 0$, Γ reell, $D > 0$,

wenn q ungerade ist, $\Gamma' = 0$, Γ rein imaginär, $D < 0$,

was die Behauptung bestätigt.

6. Sind ferner

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots, \alpha_n], \quad \mathfrak{b} = [\beta_1, \beta_2, \cdots, \beta_n]$$

zwei beliebige n-gliedrige Moduln, deren Basen zugleich Basen des Körpers sind, so läßt sich leicht übersehen, daß auch

$$\mathfrak{a} + \mathfrak{b}, \quad \mathfrak{a}\mathfrak{b}, \quad \mathfrak{a} - \mathfrak{b}, \quad \frac{\mathfrak{b}}{\mathfrak{a}}$$

ebensolche Moduln sind.

Denn erstens besteht der Modulus $\mathfrak{a} + \mathfrak{b}$ aus den Zahlen

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n + \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

ist also der endliche Modulus

$$(40) \qquad [\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_n],$$

welcher, da er n voneinander unabhängige Zahlen α_i oder β_i des Körpers enthält, nach Kap. 2, Nr. 5 auf einen n-gliedrigen reduziert werden kann, dessen unabhängige Elemente dem Körper angehören, also eine Basis desselben bilden.

Zweitens ist der Modulus $\mathfrak{a}\mathfrak{b}$ dem folgenden:

$$[\cdots, \alpha_i\beta_k, \cdots]$$

mit den für $i, k = 1, 2, \cdots, n$ gebildeten Elementen $\alpha_i\beta_k$ gleich, von welchem, da er n unabhängige Zahlen des Körpers, z. B. $\alpha_1\beta_1, \alpha_2\beta_1, \cdots, \alpha_n\beta_1$, enthält, das über den Modulus (40) Gesagte ebenfalls gilt.

Was drittens den Modulus $\mathfrak{a} - \mathfrak{b}$ betrifft, welcher die den Moduln $\mathfrak{a}, \mathfrak{b}$ gemeinsamen Zahlen umfaßt, so kann, da die Elemente β_i eine Basis des Körpers bilden, jede in $\mathfrak{a}$ enthaltene Zahl α in der Form

$$\alpha = r_1\beta_1 + r_2\beta_2 + \cdots + r_n\beta_n$$

mit rationalen Koeffizienten ausgedrückt werden; setzt man hier $r_i = \frac{\varrho_i}{\varrho}$, wo ϱ_i, ϱ ganze rationale Zahlen bedeuten, so

wird $\varrho\alpha$ eine Zahl des Modulus $\mathfrak{b}$, und somit kann jede Zahl des n-gliedrigen Modulus $\mathfrak{a}$ durch Multiplikation mit einer rationalen ganzen Zahl in eine Zahl des Modulus $\mathfrak{b}$ verwandelt werden. Infolge davon ist, wie in Kap. 2, Nr. 6 bewiesen worden ist, der Modulus $\mathfrak{a} - \mathfrak{b}$ ebenfalls ein n-gliedriger Modulus, dessen dem Körper angehörige Elemente also zugleich eine Basis des letzteren bilden.

Endlich bemerke man, um die obige Aussage auch für den Modulus $\frac{\mathfrak{b}}{\mathfrak{a}}$ zu bestätigen, daß dieser Modulus aus denjenigen Zahlen besteht, welche den Moduln

$$\mathfrak{b} \cdot \alpha_1^{-1},\ \mathfrak{b} \cdot \alpha_2^{-1},\ \cdots,\ \mathfrak{b} \cdot \alpha_n^{-1}$$

gemeinsam sind, woraus nach dem zuletzt Bewiesenen die Richtigkeit der Aussage fließt. In der Tat, damit ζ eine Zahl des Modulus $\frac{\mathfrak{b}}{\mathfrak{a}}$ sei, d. h. eine Zahl, für welche $\mathfrak{a} \cdot \zeta \succ \mathfrak{b}$ ist, ist offenbar notwendig und hinreichend, daß die Produkte

$$\alpha_1\zeta,\ \alpha_2\zeta,\ \cdots,\ \alpha_n\zeta$$

in $\mathfrak{b}$, oder daß die Zahl ζ in jedem der zuvor genannten Moduln enthalten sei.

Setzt man nun wieder spezieller voraus, daß die Moduln $\mathfrak{a}, \mathfrak{b}$ „Moduln in $\mathfrak{g}$“, ihre Basen nämlich *ganze* Zahlen des Körpers sind, so leuchtet sogleich ein, daß die Moduln $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} - \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, da sie nur aus Zahlen in $\mathfrak{g}$ bestehen, ebensolche Moduln sein müssen. Vom Modulus $\frac{\mathfrak{b}}{\mathfrak{a}}$ gilt nicht immer das Gleiche. Sind jedoch die Zahlen von $\mathfrak{b}$ im Modulus $\mathfrak{a}$ enthalten, so sind die Zahlen ζ des Modulus $\frac{\mathfrak{b}}{\mathfrak{a}}$ sämtlich ganze Zahlen, d. i. der Modulus $\frac{\mathfrak{b}}{\mathfrak{a}}$ ein „Modulus in $\mathfrak{g}$“; denn, da $\mathfrak{a}\zeta \succ \mathfrak{b}$, so ist auch $\mathfrak{a}\zeta \succ \mathfrak{a}$, also bestehen insbesondere Gleichungen von der Form

$$\begin{aligned}
\alpha_1\zeta &= g_1^{(1)}\alpha_1 + g_2^{(1)}\alpha_2 + \cdots + g_n^{(1)}\alpha_n\\
\alpha_2\zeta &= g_1^{(2)}\alpha_1 + g_2^{(2)}\alpha_2 + \cdots + g_n^{(2)}\alpha_n\\
&\cdots\cdots\cdots\cdots\cdots\\
\alpha_n\zeta &= g_1^{(n)}\alpha_1 + g_2^{(n)}\alpha_2 + \cdots + g_n^{(n)}\alpha_n
\end{aligned}$$

mit ganzzahligen Koeffizienten, aus denen ζ als eine ganze algebraische Zahl des Körpers erschlossen wird.

Aus diesem Ergebnisse folgt der Satz: Ist $\mathfrak{a}$ ein n-gliedriger Modulus des Körpers, insbesondere ein „Modulus in $\mathfrak{g}$“, so ist der Quotient

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}}$$

stets ein Modulus in $\mathfrak{g}$. Jeder Quotient dieser Art stellt wegen Kap. 2, Nr. 2 eine „Ordnung in $\mathfrak{g}$“, nämlich einen Modulus in $\mathfrak{g}$ dar, welcher die Eigenschaften einer Ordnung hat. Aber auch umgekehrt ist jede Ordnung $\mathfrak{o}$ in $\mathfrak{g}$ nach derselben Stelle der Quotient $\mathfrak{o}^0 = \frac{\mathfrak{o}}{\mathfrak{o}}$ eines Modulus in $\mathfrak{g}$.

Für jede Ordnung $\mathfrak{o}$ ganzer Zahlen des Körpers besteht die Gleichung

$$\mathfrak{g}\mathfrak{o} = \mathfrak{g}. \tag{41}$$

In der Tat, da $\mathfrak{o} \succ \mathfrak{g}$ ist, so ist auch $\mathfrak{g}\mathfrak{o} \succ \mathfrak{g}\mathfrak{g}$, d. h. $\mathfrak{g}\mathfrak{o} \succ \mathfrak{g}$; andererseits folgt aus $\mathfrak{z} \succ \mathfrak{o}$ auch $\mathfrak{z}\mathfrak{g}$ d. h. $\mathfrak{g} \succ \mathfrak{g}\mathfrak{o}$ und aus beiden Resultaten die Gleichheit (41).

Den zur Ordnung $\mathfrak{o}$ in $\mathfrak{g}$ gehörigen Quotienten

$$\mathfrak{f} = \frac{\mathfrak{o}}{\mathfrak{g}} \tag{42}$$

nennen wir mit *Dedekind* den *Führer der Ordnung* $\mathfrak{o}$.

Wegen $\mathfrak{o} \succ \mathfrak{g}$ und zufolge der letzten Bemerkung über den Quotienten zweier Moduln in $\mathfrak{g}$ ist er selbst solch ein Modulus. Da er die Gesamtheit der Zahlen ζ bedeutet, für welche $\mathfrak{g}\zeta \succ \mathfrak{o}$, so ist auch $\mathfrak{g}\mathfrak{f} \succ \mathfrak{o}$; aus $\mathfrak{z} \succ \mathfrak{g}$ folgt aber $\mathfrak{z}\mathfrak{f}$ oder

$$\mathfrak{f} \succ \mathfrak{g}\mathfrak{f},$$

also ist auch $\mathfrak{f} \succ \mathfrak{o}$. Umgekehrt ist $\mathfrak{f}\mathfrak{g} \cdot \mathfrak{g} = \mathfrak{f} \cdot \mathfrak{g}$, mithin $\mathfrak{g} \cdot \mathfrak{f}\mathfrak{g} \succ \mathfrak{o}$ und die Zahlen des Modulus $\mathfrak{f}\mathfrak{g}$ gehören folglich zu den Zahlen ζ oder es ist

$$\mathfrak{f}\mathfrak{g} \succ \mathfrak{f}.$$

Zusammen mit der vorhergefundenen, entgegengesetzten Beziehung ergibt sich die Gleichheit

$$\mathfrak{f}\mathfrak{g} = \mathfrak{f}, \tag{43}$$

der zufolge jede Zahl des ganzzahligen Modulus $\mathfrak{f}$, mit einer beliebigen ganzen algebraischen Zahl des Körpers multipliziert, wieder eine Zahl in $\mathfrak{f}$ ist. Aus all' diesem erkennt man den Satz:

Der Führer $\mathfrak{f}$ einer Ordnung $\mathfrak{o}$ in $\mathfrak{g}$ ist ein in derselben enthaltenes Ideal. Jedes andere in derselben Ordnung enthaltene Ideal $\mathfrak{j}$ ist auch enthalten in ihrem Führer $\mathfrak{f}$. Denn, da $\mathfrak{g}\mathfrak{j} \succ \mathfrak{j}$, so folgt aus $\mathfrak{j} \succ \mathfrak{o}$ auch $\mathfrak{g}\mathfrak{j} \succ \mathfrak{o}$, was nach der Bedeutung von $\mathfrak{f}$ die Beziehung $\mathfrak{j} \succ \mathfrak{f}$ nach sich zieht.

Der Führer der speziellen Ordnung $\mathfrak{g}$ ist wegen $\mathfrak{g}\mathfrak{g} = \mathfrak{g}$ offenbar $\mathfrak{g}$ selbst.

7. Sei nun

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots, \alpha_n] \tag{44}$$

ein beliebiger Modulus in $\mathfrak{g}$. Seine Basiszahlen hangen als ganze Zahlen des Körpers mit den Basiszahlen von $\mathfrak{g}$ durch n Gleichungen von der Form

$$\alpha_i = c_{i1}\gamma_1 + c_{i2}\gamma_2 + \cdots + c_{in}\gamma_n \qquad (i = 1, 2, \cdots, n) \tag{45}$$

mit ganzzahligen Koeffizienten c_{ik} zusammen. Nach Ende von Kap. 2 ist daher die Anzahl $(\mathfrak{g}, \mathfrak{a})$ der Klassen, in welche sich alle ganzen Zahlen des Körpers in bezug auf $\mathfrak{a}$ als Modulus verteilen, dem Absolutwerte der Determinante der Gleichungen (45) gleich, in Zeichen:

$$(\mathfrak{g}, \mathfrak{a}) = \pm |c_{ik}|. \tag{46}$$

Sie ist der Natur der Sache nach unabhängig von der Wahl der besonderen Basis sowohl für $\mathfrak{g}$, wie für den Modulus $\mathfrak{a}$; in der Tat, sind $\alpha_1', \alpha_2' \cdots, \alpha_n'$ irgend eine andere Basis von $\mathfrak{a}$, so bestehen Gleichungen von der Form

$$\alpha_i' = a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n, \qquad (i = 1, 2, \cdots, n)$$

deren ganzzahlige Koeffizienten a_{ik} die Determinante ± 1 haben; sind ferner $\gamma_1', \gamma_2', \cdots, \gamma_n'$ irgend eine andere Basis von $\mathfrak{g}$, so bestehen n ähnliche Gleichungen

$$\gamma_i = g_{i1}\gamma_1' + g_{i2}\gamma_2' + \cdots + g_{in}\gamma_n' \qquad (i = 1, 2, \cdots, n)$$

mit ebenfalls ganzzahligen Koeffizienten und der Determinante $|g_{ik}| = \pm 1$. Ihnen zufolge lassen sich die α_i' linear mittels der γ_i' ausdrücken durch Gleichungen mit der Determinante

$$|c_{ik}| \cdot |a_{ik}| \cdot |g_{ik}|.$$

Aus diesen Gleichungen aber erschließt man, wie (46) aus (45), die Beziehung

$$(\mathfrak{g}, \mathfrak{a}) = \pm |c_{ik}| \cdot |a_{ik}| \cdot |g_{ik}|,$$

d. i. wieder die Gleichung (46).

Die so nur durch $\mathfrak{a}$ und $\mathfrak{g}$ bestimmte Zahl $(\mathfrak{g}, \mathfrak{a})$ soll die *Norm des Modulus* $\mathfrak{a}$ genannt und mit $\mathfrak{N}(\mathfrak{a})$ bezeichnet werden, so daß

$$(47) \qquad \mathfrak{N}(\mathfrak{a}) = (\mathfrak{g}, \mathfrak{a})$$

ist. Da jedes Ideal $\mathfrak{j}$ ein Modulus in $\mathfrak{g}$ ist, so bestimmt sich nach dieser Festsetzung auch die Norm $\mathfrak{N}(\mathfrak{j})$ eines Ideals.

Wenn aber insonderheit γ irgend eine bestimmte ganze Zahl des Körpers ist, so bildet die Gesamtheit aller in $\mathfrak{g}$ enthaltenen Vielfachen von γ ein Ideal, welches das Hauptideal $\mathfrak{g}\gamma$ genannt werde, da es alle Zahlen umschließt, welche Produkte aus γ und einer Zahl in $\mathfrak{g}$ sind, und nur solche. Die Zahlen in $\mathfrak{g}$ sind aber von der Form

$$g_1\gamma_1 + g_2\gamma_2 + \cdots + g_n\gamma_n,$$

mithin diejenigen des gedachten Hauptideals die Zahlen

$$g_1 \cdot \gamma\gamma_1 + g_2 \cdot \gamma\gamma_2 + \cdots + g_n \cdot \gamma\gamma_n;$$

und da die Zahlen $\gamma\gamma_1, \gamma\gamma_2, \cdots, \gamma\gamma_n$ offenbar unabhängig voneinander sind, so sind sie Basiszahlen des Hauptideales, welche mit den Basiszahlen von $\mathfrak{g}$ durch n Gleichungen

$$(48) \qquad \gamma\gamma_i = g_{i1}\gamma_1 + g_{i2}\gamma_2 + \cdots + g_{in}\gamma_n \quad (i = 1, 2, \cdots, n)$$

mit ganzzahligen Koeffizienten verbunden sein müssen. Hieraus folgt nach den unmittelbar vorhergehenden Sätzen für die Norm des Hauptideals $\mathfrak{g}\gamma$ die Beziehung

$$\mathfrak{N}(\mathfrak{g}\gamma) = \pm |g_{ik}|.$$

Bedenkt man aber, daß die γ_i auch eine Basis des Körpers ausmachen, vergleicht man ferner die Gleichungen (48) mit den Formeln (32) des ersten Kapitels und erinnert sich der dort in (38) gegebenen Definition der Norm einer Zahl, so folgert man schließlich die Gleichung

$$(49) \qquad \mathfrak{N}(\mathfrak{g}\gamma) = \pm N(\gamma).$$

Auch jede Ordnung in $\mathfrak{g}$ ist ein besonderer Modulus in $\mathfrak{g}$. Bezeichnen $\omega_1, \omega_2, \cdots, \omega_n$ Basiszahlen der Ordnung $\mathfrak{o}$, so bestehen n Gleichungen

$$\omega_i = k_{i1}\gamma_1 + k_{i2}\gamma_2 + \cdots + k_{in}\gamma_n \tag{50}$$
$$(i = 1, 2, \cdots, n)$$

mit ganzzahligen Koeffizienten, deren Determinante nach ihrem Absolutwerte k heiße:

$$k = \pm |k_{ih}|. \tag{51}$$

Die Norm

$$\mathfrak{N}(\mathfrak{o}) = (\mathfrak{g}, \mathfrak{o}) \tag{52}$$

der Ordnung oder die Anzahl der Klassen kongruenter Zahlen, in welche sich alle ganzen Zahlen des Körpers in bezug auf die Ordnung als Modulus verteilen, ist diesem Absolutwerte gleich, in Zeichen:

$$(\mathfrak{g}, \mathfrak{o}) = k. \tag{53}$$

Endlich ergibt sich aus (50) das k-fache jeder der Basiszahlen von $\mathfrak{g}$ und somit auch das k-fache jeder ganzen Zahl des Körpers als eine Zahl der Ordnung, d. h. das Hauptideal $\mathfrak{g}k$ ist in $\mathfrak{o}$ enthalten, woraus nach der vorigen Nummer hervorgeht, daß es auch im Führer der Ordnung enthalten sein muß:

$$\mathfrak{g}k \succ \mathfrak{f}. \tag{54}$$

Fünftes Kapitel.

Die Entwicklung der Theorie am Beispiel des quadratischen Körpers erläutert.

1. Bevor wir nun in der Darstellung der allgemeinen Theorie fortfahren, wollen wir einen besonderen Zahlenkörper, den sogenannten quadratischen, in Betracht ziehen. Es wird nicht beabsichtigt, hier eine vollständige Theorie desselben zu geben, die vielmehr der Fortsetzung dieses Werks vorbehalten bleiben muß; wir gedenken nur, indem wir an diesem Beispiele die eingeführten Begriffe dem Leser vertrauter machen wollen, zugleich in kurzen Zügen die wesentlichen Stadien

darzulegen, durch welche die geschichtliche Entwicklung unserer Theorie hindurchgegangen ist, bis sie ihren heutigen festgegründeten und allumfassenden Stand erreicht hat.

Unter einem quadratischen Körper versteht man jeden endlichen Körper $K(\mathsf{A}; R)$ zweiten Grades, d. i. einen Körper, der von der Wurzel A einer irreduktibeln quadratischen Gleichung

$$f(x) = ax^2 + bx + c = 0 \tag{1}$$

mit ganzzahligen Koeffizienten a, b, c erzeugt wird. Die Gesamtheit seiner Zahlen liefert die Formel

$$\eta = r + s\mathsf{A}, \tag{2}$$

wenn unter r, s alle rationalen Zahlen verstanden werden, während

$$\mathsf{A} = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

ist. Man kann

$$b^2 - 4ac = \beta^2 \cdot d \tag{3}$$

setzen, indem man unter d eine ganze Zahl ohne quadratischen Teiler versteht: sie darf aber weder Null noch Eins sein, da sonst die Gleichung (1), welche als irreduktibel vorausgesetzt worden, rationale Wurzeln besitzen und $f(x)$ in zwei rationale Linearfaktoren zerlegbar sein würde. Hierdurch nimmt die Formel (2) die Gestalt an:

$$\zeta = p + q\sqrt{d}, \tag{4}$$

wo wieder p, q alle rationalen Zahlen bedeuten. Es handelt sich vor allem darum, die ganzen algebraischen Zahlen des Körpers aus dieser Allgemeinheit seiner sämtlichen Zahlen auszuscheiden. Man setze $p = \frac{p_0}{n_0}$, $q = \frac{q_0}{n_0}$, indem man mit n_0 den Generalnenner der beiden rationalen Zahlen p, q bezeichnet, so daß p_0, q_0, n_0 drei ganze Zahlen ohne gemeinsamen Teiler bedeuten. Dann folgt aus (4) für ζ die quadratische Gleichung

$$\zeta^2 - \frac{2p_0}{n_0} \cdot \zeta + \frac{p_0^2 - dq_0^2}{n_0^2} = 0$$

und es handelt sich darum, p_0, q_0, n_0 so zu wählen, daß ihre Koeffizienten ganzzahlig werden. Dazu muß, wenn unter P, Q ganze Zahlen verstanden werden,

(5) $$2p_0 = n_0 \cdot P, \quad p_0^2 - dq_0^2 = n_0^2 \cdot Q$$

werden. Wäre nun zuerst n_0 ungerade, so müßte $P = 2P'$ und $p_0 = n_0 P'$ sein, aus der zweiten der voraufgehenden Gleichungen folgte dq_0^2 teilbar durch n_0^2 und, da q_0 keinen Teiler mit p_0, n_0 gemeinsam, d aber keinen quadratischen Teiler haben kann, muß $n_0 = 1$, folglich

$$\xi = p_0 + q_0\sqrt{d}$$

sein. Wird dagegen n_0 gerade gedacht, etwa $n_0 = 2\nu$, so ergibt sich aus (5)

$$p_0 = \nu \cdot P, \quad dq_0^2 \text{ teilbar durch } \nu^2,$$

also wieder $\nu = 1$ und $n_0 = 2$; dann gibt aber die zweite der Gleichungen (5) die Kongruenz

$$p_0^2 - dq_0^2 \equiv 0 \pmod{4},$$

aus welcher, da d nicht durch 4 teilbar ist, p_0 und q_0 aber nicht zugleich mit n_0 gerade sein können, die Zahlen p_0, q_0 sich als ungerade und folglich sich

$$\xi = \frac{p^0 + q^0\sqrt{d}}{2}$$

mit ungeraden Elementen p^0, q^0 und

$$d \equiv 1 \pmod{4}$$

ergibt. Der letzte Fall ereignet sich demnach nur dann, wenn d von der Form $4k + 1$ ist. Man gelangt so zu folgendem Endergebnis:

Die ganzen Zahlen des quadratischen Körpers werden gegeben durch die Formel

$$\xi = p_0 + q_0\sqrt{d}$$

mit beliebigen ganzzahligen Elementen p_0, q_0, wenn $d \equiv 2, 3 \pmod{4}$ ist, dagegen, wenn $d \equiv 1 \pmod{4}$ ist, außer durch diese Formel noch durch die zweite:

$$\xi = \frac{p_0 + q_0\sqrt{d}}{2}$$

mit ungeraden Elementen p_0, q_0, oder, was dasselbe sagt, durch die eine Formel

$$\xi = \frac{p_0 + q_0\sqrt{d}}{2},$$

deren ganzzahlige Elemente p_0, q_0 gleichartig gedacht sind:

$$p_0 \equiv q_0 \pmod{2}.$$

Setzt man im letzteren Falle $p_0 = 2z + q_0$, so wird

$$\zeta = z \cdot 1 + q_0 \cdot \frac{1+\sqrt{d}}{2},$$

und da übrigens p_0, q_0 im ersten Falle, z, q_0 im zweiten Falle beliebige ganze Zahlen bedeuten, darf man sagen: die ganzen Zahlen des quadratischen Körpers sind die Zahlen des Modulus

$$\mathfrak{g} = [1, \sqrt{d}], \tag{6}$$

wenn $d \equiv 2, 3 \pmod{4}$, dagegen die Zahlen des Modulus

$$\mathfrak{g} = \left[1, \frac{1+\sqrt{d}}{2}\right], \tag{7}$$

wenn $d \equiv 1 \pmod{4}$ ist. Im ersten Falle sind demnach $\gamma_1 = 1$, $\gamma_2 = \sqrt{d}$, im zweiten $\gamma_1 = 1$, $\gamma_2 = \frac{1+\sqrt{d}}{2}$ Basiszahlen von $\mathfrak{g}$. Da nun offenbar die zur Zahl (4) konjugierte Zahl erhalten wird, indem man $\sqrt{d}$ in $-\sqrt{d}$ verwandelt, so ist im ersten Falle

$$\Delta(\gamma_1, \gamma_2) = \begin{vmatrix} 1, & \sqrt{d} \\ 1, & -\sqrt{d} \end{vmatrix}^2 = 4d,$$

im zweiten Falle

$$\Delta(\gamma_1, \gamma_2) = \begin{vmatrix} 1, & \frac{1+\sqrt{d}}{2} \\ 1, & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d;$$

die Grundzahl des quadratischen Körpers ist daher

$$\begin{cases} \mathrm{D} = 4d, & \text{wenn } d \equiv 2, 3 \pmod{4} \\ \mathrm{D} = d, & \text{wenn } d \equiv 1 \pmod{4}. \end{cases} \tag{8}$$

Man übersieht hiernach leicht, daß in beiden Fällen gesetzt werden darf

$$\mathfrak{g} = \left[1, \frac{\mathrm{D}+\sqrt{\mathrm{D}}}{2}\right]. \tag{9}$$

Die Formel (6) bezw. (7), welche die ganzen Zahlen des aus der Wurzel A der quadratischen Gleichung (1) entstehenden

Körpers $K(\mathsf{A};\,R)$ gibt, liefert ebenso auch die ganzen Zahlen des Körpers $K(\sqrt{d};\,R)$; da nämlich wegen (3)

$$\mathsf{A} = \frac{-b+\beta\sqrt{d}}{2a},$$

also umgekehrt

$$\sqrt{d} = \frac{2a\cdot\mathsf{A}+b}{\beta},$$

jede der beiden Zahlen A, $\sqrt{d}$ also rational durch die andere ausdrückbar oder in dem aus der anderen gebildeten Körper enthalten ist, so ist auch jeder dieser zwei Körper selbst im andern enthalten, also

$$K(\mathsf{A};\,R) = K(\sqrt{d};\,R).$$

Hiernach ist insbesondere, wenn $d=-1$, d. i. $\sqrt{d}=i$ gedacht wird, die Gesamtheit der ganzen Zahlen des Körpers $K(i;\,R)$ der Modulus

$$\mathfrak{g} = [1,\,i],$$

d. i. die Gesamtheit der sogenannten komplexen ganzen Zahlen von der Form $x+yi$ mit ganzzahligen Elementen x, y, und die Grundzahl dieses Körpers ist $\mathrm{D}=-4$.

Ist dagegen $d=-3$ mithin $\mathrm{D}=d=-3$, so ist nach (9) die Gesamtheit der ganzen Zahlen des Körpers $K(\sqrt{-3};\,R)$ nicht der Modulus $[1,\sqrt{-3}]$, sondern der Modulus

$$\mathfrak{g} = \left[1,\,\frac{-3+\sqrt{-3}}{2}\right],$$

wofür auch der Modulus $[1,\,\varrho]$ gesetzt werden kann, wenn unter ϱ die imaginäre kubische Einheitswurzel

$$\varrho = \frac{-1+\sqrt{-3}}{2}$$

verstanden wird; sie ist also nicht diejenige der Zahlen von der Form $x+y\sqrt{-3}$, sondern die Gesamtheit der sogenannten komplexen ganzen Zahlen von der Form $x+y\varrho$, von welcher die erstere nur einen Teil ausmacht.

2. Die Theorie der komplexen ganzen Zahlen von der Form $x+yi$ ist das früheste Beispiel von der Arithmetik eines Zahlenkörpers, welches behandelt worden ist. Nachdem

Gauß[1]) die reale Bedeutung der komplexen Größen festgestellt und in seinem Fundamentalsatze, daß für jede algebraische Gleichung im Gebiete dieser Größen eine Wurzel existiere, ihre Wichtigkeit für die Theorie der Gleichungen, sowie bald hernach auch für die Theorie der elliptischen Funktionen erkannt hatte, fand er andererseits bei seinen Bemühungen, die Theorie der biquadratischen Reste[2]) auf ähnliche Gesetze zurückzuführen, wie sie in derjenigen der quadratischen Reste bestehen, daß dies nur möglich werde, wenn neben den reellen ganzen Zahlen auch die komplexen ganzen Zahlen $x + yi$ in die Betrachtung gezogen würden. Dies gab die Veranlassung, zunächst die Teilbarkeitsgesetze der letzteren zu untersuchen, was schon von Gauß selbst, später dann von Dirichlet in seiner Abhandlung: recherches sur les formes quadratiques à coefficiens et à indéterminées complexes, Journ. f. Math. 24, S. 291 getan worden ist. Hierbei stellte sich der wichtige Umstand heraus, daß für solche komplexe Zahlen ein ganz analoger Algorithmus aufgestellt werden könne, wie der Euclidische Algorithmus zur Auffindung des größten gemeinsamen Teilers zweier reellen ganzen Zahlen, der nun, ganz wie der letztere, die Quelle darbietet, um völlig der reellen Zahlentheorie entsprechende Sätze über die Teilbarkeit der komplexen Zahlen, ihre eindeutige Zerlegbarkeit in Primfaktoren u. dgl. m. zu erlangen. Versteht man unter der Norm $N(x + yi)$ der komplexen Zahl $x + yi$ das Produkt

$$(x + yi)(x - yi) = x^2 + y^2$$

der beiden konjugierten Zahlen $x + yi$, $x - yi$, so ist die wesentliche Grundlage der ganzen Theorie der einfache Satz, daß für jede komplexe Größe $z = x + yi$ eine komplexe ganze Zahl $m = a + bi$ angebbar ist, für welche

$$N(z - m) < 1 \tag{10}$$

ist.

1) S. Gauß' Anzeige seiner theoria residuorum biquadraticorum, commentatio secunda, in Göttinger gel. Anz. 1831, April 23 (Gauß' Werke 2, p. 169); ferner die Abhandlungen in Gauß' W. 3, p. 1, 31, 57.

2) Gauß' theoria resid. biquadr., comment. secunda, Comment. Gotting. rec. 7, 1832 oder Gauß' Werke 2, p. 93.

Diese Gaußischen Erfolge legten es Eisenstein und Jacobi[1]) bei ihren Untersuchungen über kubische Reste nahe, die Theorie derselben auf die Arithmetik einer geeigneten entsprechenden Gattung komplexer Zahlen zu begründen. Als solche erwies sich die Gattung der Zahlen von der Form

$$x + y\varrho,$$

worin $\varrho = \frac{-1+\sqrt{-3}}{2}$ eine kubische Einheitswurzel ist, und für welche in der Tat ein der Formel (10) völlig entsprechender Satz und damit ein Euclidischer Algorithmus vorhanden ist. Auf Grund des letztern ergaben sich dann wieder für diese neue Gattung komplexer ganzer Zahlen genau die gleichen Teilbarkeitsgesetze, die für die reelle Zahlentheorie und diejenige der Zahlen $x + yi$ bereits festgestellt waren. In der Tat darf man allgemein aussagen, daß, so oft für eine Gattung von algebraischen Zahlen ein Euclidischer Algorithmus nachweisbar ist, sicher ganz analoge Gesetze der Teilbarkeit werden gelten müssen, wie in der gewöhnlichen Zahlentheorie, wobei freilich zu beachten ist, daß jene ausreichende Bedingung nicht auch notwendig zu sein braucht.

In der Erwartung ähnlich einfacher aber allgemeinerer Ergebnisse, wie in den beiden bisher besprochenen Gebieten der aus i oder aus ϱ, d. h. aus gewissen Einheitswurzeln zusammengesetzten komplexen ganzen Zahlen, unternahmen es nunmehr Dirichlet und Kummer, die Zahlengattungen zu untersuchen, die aus einer beliebigen Einheitswurzel und ganzzahligen Koeffizienten zusammengesetzt sind, bei denen allgemein ein Euclidischer Algorithmus nicht mehr besteht. Von des Ersteren Untersuchungen sind nur die wichtigen Sätze bekannt geworden, durch welche die Gesamtheit aller Einheiten eines solchen Zahlengebietes bestimmt und auf eine endliche Anzahl sogenannter Fundamentaleinheiten zurück-

---

3) Jacobi, über die Kreisteilung und ihre Anwendung auf die Zahlentheorie, Berliner Monatsber. 1837 oder Journ. f. Math. 30, p. 166; Eisenstein, Beweis des Reziprozitätsgesetzes für die kubischen Reste, Journ. f. Math. 27, p. 289. S. auch Lebesgue, recherches sur les nombres, Liouville's Journ. d. Math. 4.

geführt wird.[1]) Wie bedeutend diese schönen Dirichletschen Ergebnisse auch waren, folgenreicher wurde der Umstand, zu welchem sich Kummer geführt sah und den er in einer akademischen Gelegenheitsschrift (de numeris complexis, qui radicibus unitatis et numeris integris realibus constant, Vratislaviae, 1844) bekannt gemacht hat, der Umstand nämlich, daß in einem solchen Gebiete zwar eine endliche aber nicht mehr eine eindeutige Zerlegbarkeit der Zahlen in unzerlegbare Faktoren stattfindet. Diese fatale Tatsache schien jede Möglichkeit zu benehmen, jemals die Teilbarkeitsgesetze für derartige Zahlengebiete in ähnlicher Einfachheit und Schönheit formulieren zu können, wie in den früher betrachteten Gattungen ganzer Zahlen.[2]) Aber gerade sie sollte der Keim werden, aus welchem der Zahlentheorie ein ganz neuer fruchtbringender Begriff und damit eine ungeahnte weitere Ausgestaltung herauswuchs. Die Bemühungen Kummers, jene Schwierigkeit der neuen Theorie zu überwinden, führten ihn zu dem genialen Gedanken einer Neuschöpfung geeigneter Zahlen, die er ideale Zahlen benannt hat.[3]) Wie diese Zahlen in dem gedachten Zahlengebiete zu verstehen und einzuführen sind, kann hier nicht auseinandergesetzt werden; man findet das Wesentliche darüber dargestellt in des Verfassers Werke: Die Lehre von der Kreisteilung usw. 1872, 17. und 18. Vorlesung. Der Begriff und die Verwendung der idealen Zahlen Kummers läßt sich jedoch ebensogut auch erläutern am Beispiele des quadratischen Körpers, mit dem wir uns hier beschäftigen und bei welchem im allgemeinen ebenfalls jene Erscheinung der nicht mehr eindeutigen Zerlegbarkeit der Zahlen in einfachste Faktoren bemerkbar ist.

---

1) Dirichlet, Berl. Monatsber. 1841, 1842, 1846 und Par. C. R 1840, 10, p. 286.

2) Kummer selbst spricht a. a. O. darüber sich folgendermaßen aus: Maxime dolendum videtur, quod haec numerorum realium virtus, ut in factores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quae, si esset, tota haec doctrina, quae magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset.

3) Seine bezüglichen Arbeiten finden sich hauptsächlich im Journ. f. Math. 30, 35, 40, in Liouv. Journ. de Math. 16, sowie in den Abhh. der Berliner Akademie 1856, 1857, 1859, 1861.

3. Beschränken wir uns aber bei diesen Betrachtungen der Einfachheit wegen auf den Fall, in welchem

$$d \equiv -1 \pmod{4},$$

also die Gesamtheit $\mathfrak{g}$ der ganzen Zahlen des quadratischen Körpers der Modulus $[1, \sqrt{d}]$ und $4d$ die Grundzahl des Körpers ist.

Eine ganze Zahl des Körpers d. i. eine Zahl $x + y\sqrt{d}$ mit ganzzahligen x, y heißt durch eine andere ganze Zahl $x' + y'\sqrt{d}$ desselben teilbar, wenn eine dritte ganze Zahl $x'' + y''\sqrt{d}$ desselben vorhanden ist, für welche

$$(11) \qquad x + y\sqrt{d} = (x' + y'\sqrt{d})(x'' + y''\sqrt{d})$$

ist. Aus dieser Beziehung folgt dann die gleiche Beziehung zwischen den konjugierten Zahlen

$$(12) \qquad x - y\sqrt{d} = (x' - y'\sqrt{d})(x'' - y''\sqrt{d})$$

und daher auch die entsprechende Beziehung zwischen ihren Normen:

$$(13) \qquad N(x + y\sqrt{d}) = N(x' + y'\sqrt{d}) \cdot N(x'' + y''\sqrt{d}).$$

Ist nun auch umgekehrt $x' + y'\sqrt{d}$ teilbar durch $x + y\sqrt{d}$, sodaß

$$x' + y'\sqrt{d} = (x + y\sqrt{d}) \cdot (x_2 + y_2\sqrt{d})$$

gesetzt werden kann, so gibt die Verbindung dieser Formel mit der Formel (11) die Gleichheit

$$(14) \qquad 1 = (x'' + y''\sqrt{d}) \cdot (x_2 + y_2\sqrt{d})$$

d. h. $x'' + y''\sqrt{d}$ ist ein Teiler der Einheit und deshalb auch ein Teiler jeder ganzen Zahl des Körpers, eine sogenannte Einheit des Körpers. Da aus (14) durch den Übergang zu den Normen

$$1 = N(x'' + y''\sqrt{d}) \cdot N(x_2 + y_2\sqrt{d})$$

gefunden wird, so muß die Norm jeder Einheit, da sie wegen $d \equiv -1 \pmod{4}$ nicht -1 sein kann, gleich 1 sein, wie denn auch umgekehrt jede Zahl $x'' + y''\sqrt{d}$, deren Norm 1 ist, eine Einheit des Körpers ist. Zwei Zahlen $x + y\sqrt{d}$, $x' + y'\sqrt{d}$, welche sich nur um einen Faktor unterscheiden, welcher eine Einheit ist, derart, daß in (11)

$$N(x'' + y''\sqrt{d}) = 1$$

ist, werden assoziierte Zahlen genannt.

Da jede Norm

$$N(x + y\sqrt{d}) = x^2 - dy^2$$

eine rationale ganze Zahl ist, so erkennt man hiernach mit Rücksicht auf (13), daß, wenn eine Zahl $x + y\sqrt{d}$ zerlegbar, nämlich das Produkt zweier Faktoren ist, deren keiner eine Einheit, auch ihre Norm eine im gewöhnlichen Sinne zerlegbare rationale ganze Zahl ist. Demnach werden alle diejenigen Zahlen $x + y\sqrt{d}$ unzerlegbar sein, deren Norm

$$N(x + y\sqrt{d}) = p \tag{15}$$

eine rationale Primzahl ist; aber das Umgekehrte braucht nicht der Fall zu sein. Z. B. ist, wenn $d = -5$,

$$N(\mp 1 + 2\sqrt{-5}) = 21 = 3.\ 7$$

und doch, wie man sich unschwer überzeugt, die Zahl $-1 + 2\sqrt{-5}$ auf keine Weise in ein Produkt zweier Zahlen $x' + y'\sqrt{-5}$, $x'' + y''\sqrt{-5}$, welche von Einheiten verschieden sind, zerlegbar. So oft nun für eine unzerlegbare Zahl $x + y\sqrt{d}$ die Norm

$$N(x + y\sqrt{d}) = m \cdot n$$

eine zusammengesetzte Zahl ist, so oft tritt offenbar die gedachte Erscheinung einer mehrfachen Zerlegung derselben Zahl in unzerlegbare Faktoren zutage. Es fragt sich dann, wie man zur Eindeutigkeit der Zerlegung hier wieder zurück gelangen kann.

Offenbar müssen die wahren Primfaktoren von $x + y\sqrt{d}$ da sie auch in der Norm $N(x + y\sqrt{d})$ aufgehen, in den rationalen Primzahlen aufgehen, aus denen diese sich zusammensetzt. Untersuchen wir daher zunächst, wann und auf welche Weise eine gegebene Primzahl p in der Norm einer komplexen ganzen Zahl $x + y\sqrt{d}$ aufgehen oder die Kongruenz

$$x^2 - dy^2 \equiv 0 \pmod{p} \tag{16}$$

bestehen kann. Man muß hierzu durchaus unterscheiden, ob die Primzahl p die Grundzahl $4d$ des Körpers teilt oder nicht. Geht zunächst p in $4d$ nicht auf, so kann d bezüglich dieser

ungeraden Primzahl p entweder quadratischer Rest oder Nichtrest sein. Im erstern Falle hat die Kongruenz

$$(17) \qquad z^2 \equiv d \pmod{p}$$

zwei einander entgegengesetzte Wurzeln, welche w und $-w$ heißen mögen. Da somit $w^2 \equiv d \pmod{p}$ ist, nimmt die Kongruenz (16) die Gestalt

$$\left.\begin{aligned} x^2 - w^2y^2 &\equiv 0 \\ \text{oder} \qquad (x+wy)(x-wy) &\equiv 0 \end{aligned}\right\} \pmod{p}$$

an und mindestens einer dieser Faktoren muß teilbar sein durch p. Wären sie es beide, so wären es auch $2x$ und $2wy$, d. h. x und y, und die komplexe Zahl $x + y\sqrt{d}$ hätte den Teiler p. Andernfalls kann nur ein bestimmter der beiden Faktoren durch p aufgehen, und hier setzt nun Kummers neue Begriffsbildung ein. Wenn nämlich $x + wy$ durch p teilbar ist, so soll nach seinem Vorgange gesagt werden: die Zahl $x + y\sqrt{d}$ enthalte einen idealen Faktor von p, der durch die Kongruenzwurzel w charakterisiert ist und deshalb der zur Kongruenzwurzel w gehörige ideale Faktor von p heißen und durch (p, w) bezeichnet werden soll. Ist im Gegenteil $x - wy$ teilbar durch p, so enthält $x + y\sqrt{d}$ den zur Wurzel $-w$ gehörigen idealen Faktor $(p, -w)$ von p. Findet beides statt, so ist, wie schon bemerkt, $x + y\sqrt{d}$ teilbar durch p, und somit darf p selbst als das Produkt der beiden „konjugierten" idealen Faktoren (p, w), $(p, -w)$ aufgefaßt und die Norm

$$(18) \qquad N(p, w) = N(p, -w) = (p, w) \cdot (p, -w) = p$$

gesetzt werden.

Man erkennt nun vor allem, daß die so definierten idealen Faktoren von p Primfaktoren sind, nämlich der Eigenschaft genießen, daß ein Produkt zweier komplexen Zahlen nur dann durch einen solchen Faktor teilbar ist, wenn ihn eine dieser Zahlen enthält. In der Tat, enthielte das Produkt

$$(x + y\sqrt{d}) \cdot (x' + y'\sqrt{d}) = xx' + dyy' + (xy' + x'y)\sqrt{d}$$

den idealen Faktor (p, w), so müßte

d. i.
$$\left.\begin{aligned} xx' + dyy' + (xy' + x'y)\,w \equiv 0 \\ (x + wy)(x' + wy') \equiv 0 \end{aligned}\right\} \pmod{p},$$

also einer der Faktoren durch p und die entsprechende der Zahlen $x + y\sqrt{d}$, $x' + y'\sqrt{d}$ durch (p, w) teilbar sein. Weil die Normen dieser Primfaktoren gleich p^1 sind, sollen sie selbst ideale Primzahlen ersten Grades genannt werden.

Aus der Möglichkeit der Kongruenz (17) folgt bekanntlich auch diejenige der Kongruenz

$$z^2 \equiv d \pmod{p^m}, \tag{19}$$

die wieder zwei einander entgegengesetzte Wurzeln w_m, $-w_m$ hat; unter ihnen sei w_m diejenige, welche mit $w \pmod{p}$ kongruent ist. Dann ist nach Kummer weiter zu definieren: die Zahl $x + y\sqrt{d}$ enthalte den idealen Primfaktor (p, w) m Mal, wenn

$$x + w_m y \equiv 0 \pmod{p^m} \tag{20}$$

ist, und genau m Mal, wenn dann nicht mehr

$$x + w_{m+1} y \equiv 0 \pmod{p^{m+1}}$$

ist. Hieraus ergibt sich leicht die Folgerung, daß eine Zahl $x + y\sqrt{d}$, welche diesen idealen Primfaktor m Mal enthält, ihn auch $m - 1$ Mal u. s. w. enthalten muß, denn aus (20) folgt

$$x + w_m y \equiv 0 \pmod{p^{m-1}}$$

und daher auch

$$x + w_{m-1} y \equiv 0 \pmod{p^{m-1}},$$

da $w_m \equiv w_{m-1} \pmod{p^{m-1}}$ sein muß.

Ist auf solche Weise jede ungerade Primzahl p, für welche $\left(\frac{d}{p}\right) = 1$ ist, als Produkt zweier konjugierter idealer Zahlen ersten Grades dargestellt, so sieht man sogleich ein, daß jede ungerade Primzahl p, für welche $\left(\frac{d}{p}\right) = -1$ ist, in der gegenwärtigen Theorie selbst eine Primzahl ist. In der Tat ist die Kongruenz (16) in diesem Falle nur möglich, wenn y und folglich auch x durch p teilbar ist. Demnach geht ein Produkt

(21) $(x + y\sqrt{d})(x' + y'\sqrt{d}) = xx' + dyy' + (xy' + x'y)\sqrt{d}$

durch p nur auf, wenn einer der Faktoren es tut, da aus

$$xx' + dyy' \equiv 0, \quad xy' + x'y \equiv 0 \pmod{p}$$

sich nach der Formel

$$(x^2 - dy^2)(x'^2 - dy'^2) = (xx' + dyy')^2 - d(xy' + x'y)^2$$

eine der Kongruenzen

$$x^2 - dy^2 \equiv 0, \quad x'^2 - dy'^2 \equiv 0 \pmod{p}$$

erfüllt, mithin eine der Zahlen $x + y\sqrt{d}$, $x' + y'\sqrt{d}$ sich durch p teilbar erweist. Eine solche Primzahl heißt zweiten Grades, da ihre Norm $N(p) = p^2$ ist.

Es bleiben noch zu betrachten die in der Grundzahl $4d$ aufgehenden Primzahlen, also die Zahl 2 und die ungeraden Primzahlen q, aus denen sich d zusammensetzt. Damit zunächst

$$x^2 - dy^2 \equiv 0 \pmod{q}$$

sei, ist die Bedingung

(22) $$x \equiv 0 \pmod{q}$$

erforderlich und genügend. Findet sie statt, so soll gesagt werden, die komplexe Zahl $x + y\sqrt{d}$ enthalte einen idealen Faktor von q, welcher durch k ausgedrückt werde. Derselbe zeigt sich sogleich als ein Primfaktor kraft der Eigenschaft, nach welcher ein Produkt (21) zweier komplexen Zahlen ihn nur dann enthalten kann, wenn $xx' + dyy'$, d. h. wenn xx', also mindestens eine der beiden Zahlen x, x' durch q, oder eine der beiden komplexen Zahlen durch k teilbar ist. Da, wenn beide Zahlen diesen Faktor enthalten, nach (21) ihr Produkt einerseits durch k^2, andererseits durch q aufgeht, darf man sagen, daß q mit dem Quadrate des idealen Primfaktors k identisch,

(23) $$q = k^2$$

sei, der seinerseits nach der Beziehung

$$q^2 = N(q) = N(k^2) = N(k)^2$$

oder $q = N(k)$ sich als eine Primzahl ersten Grades herausstellt.

Ganz ähnlich erkennt man als notwendige und hinreichende Bedingung für das Stattfinden der Kongruenz

$$x^2 - dy^2 \equiv 0 \pmod{2}$$

die Kongruenz

$$x \equiv y \pmod{2}. \tag{24}$$

Ist sie erfüllt, so soll gesagt werden, $x + y\sqrt{d}$ enthalte einen idealen Faktor von 2. Auch dieser ist wieder ein Primfaktor, da er das Produkt (21) nur teilen kann, wenn

$$\left.\begin{aligned} xx' + dyy' &\equiv xy' + x'y \\ \text{oder} \qquad (x-y)(x'-y') &\equiv 0 \end{aligned}\right\} \pmod{2}$$

ist, was entweder $x \equiv y$ oder $x' \equiv y'$, d. h. die Teilbarkeit von $x + y\sqrt{d}$ oder $x' + y'\sqrt{d}$ durch jenen Faktor ergibt. Die Zahl 2 ist wieder als das Quadrat desselben zu betrachten, da, wenn beide Zahlen $x + y\sqrt{d}$, $x' + y'\sqrt{d}$ den Primfaktor enthalten, ihr Produkt einerseits als durch jenes Quadrat teilbar anzusehen, andererseits wegen (21) durch 2 teilbar ist. Somit erweist sich der Primfaktor von 2 auch wieder als eine Primzahl ersten Grades.

Die Teilbarkeit endlich einer Zahl $x + y\sqrt{d}$ durch eine höhere Potenz dieses Primfaktors oder der idealen Zahl k läßt sich ähnlich definieren, wie für die idealen Primfaktoren der zuerst betrachteten Primzahlen p, worauf hier nicht näher eingegangen werden soll. Es ist nun aber auch leicht einzusehen, was darunter zu verstehen ist, wenn eine Zahl $x + y\sqrt{d}$ durch ein Produkt P gegebener, idealer Primfaktoren teilbar genannt wird; sie hat dann eben nur die Reihe von Kongruenzen, welche ihre Teilbarkeit durch die Potenzen der einzelnen dieser Primfaktoren definieren, insgesamt zu erfüllen. Im allgemeinen wird es hierbei keine wirkliche komplexe Zahl geben, die diesem Produkte als gleich zu achten ist, P vielmehr selbst als ideale Zahl zu betrachten sein; dagegen hat man

$$x + y\sqrt{d} = P$$

zu setzen, wenn unter P das Produkt der sämtlichen idealen Primfaktoren verstanden wird, welche in $x + y\sqrt{d}$ aufgehen. Um dies Produkt zu finden, hat man nur die Norm $N(x + y\sqrt{d}) = x^2 - dy^2$ in ihre rationalen Primzahlpotenzen,

diese wieder in die entsprechenden Potenzen ihrer idealen Primfaktoren zu zerlegen und nach den angegebenen Regeln festzustellen, welche dieser Faktoren und wie oft ein jeder von ihnen in $x + y\sqrt{d}$ nachweisbar ist; das Produkt der so festgestellten Potenzen idealer Primfaktoren ist P. Da nun die Norm $x^2 - dy^2$ nur eine endliche Anzahl rationaler Primfaktoren besitzt, so ersieht man, daß jede komplexe Zahl als aus einer endlichen Anzahl idealer Primfaktoren zusammengesetzt oder als deren Produkt angesehen werden kann, und überzeugt sich aus der Primzahlennatur dieser idealen Faktoren ohne Mühe, daß jede solche Zerlegung einer komplexen Zahl in ideale Primfaktoren auch eine eindeutige ist.

Dies mag genügen, um den genialen Grundgedanken Kummers und den von ihm geschaffenen Begriff idealer Zahlen am Beispiele des quadratischen Körpers zu erläutern und das wichtigste Ergebnis, um deswillen dieser Begriff eingeführt worden ist, hier anzuzeigen. Man bemerke dabei, daß die idealen Zahlen nur insofern ideal, d. h. allgemein im Gebiete der komplexen ganzen Zahlen von der Form $x + y\sqrt{d}$ nicht wirklich vorhanden zu benennen sind, als man sie eben als Zahlen oder Faktoren vorstellen will, daß ihnen dagegen durchaus ein reales Substrat zukommt, wenn man von dieser Vorstellung absieht, nämlich das Stattfinden gewisser, ihnen entsprechender Kongruenzen. Es findet hier, wie Kummer treffend es ausgedrückt hat, ein ganz ähnliches Verhältnis statt, wie in der Chemie, in welcher auch gewisse Elemente, die als solche für sich isoliert nicht darstellbar sind, gleichwohl in Verbindung mit anderen durch chemische Reaktionen, die nur ihnen eigentümlich sind, ihr Vorhandensein kundgeben.

4. Wie gesagt, hat Kummer selbst seinen neuen Gedanken durchgeführt in der Theorie des Kreisteilungskörpers, d. h. der komplexen Zahlen, welche aus rationalen ganzen Zahlen und Wurzeln der Einheit zusammengesetzt sind. Der glückliche Erfolg seiner Neuschöpfung führte dann dazu, sie auch für andere Zahlengebiete nutzbar zu machen. So hat L. Fuchs (im Journ. f. Math. 61 und 65) die Kummersche Theorie der

Kreisteilungskörper für den Fall der Einheitswurzeln von beliebigem statt von einem Primzahlgrade weitergeführt; so hat der Verfasser die Theorie der komplexen Zahlen entwickelt, welche aus zwei Quadratwurzeln gebildet sind, und damit eine Arbeit Dirichlets in anderer Fassung verallgemeinert; die gleiche Theorie für Zahlen, die aus drei Quadratwurzeln gebildet sind, findet sich bei Göring.[1]) Eine auf kubische Körper bezügliche Arbeit sind Eisensteins „allgemeine Untersuchungen der Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken" (Journ. f. Math. 28, p. 289 und 29, p. 19). Bei all' diesen Anwendungen des Kummerschen Gedankens waren eigentlich prinzipielle Schwierigkeiten nicht mehr zu überwinden. Auf solche aber stieß man, als man nun den Versuch machte, auf der gleichen Grundlage allgemein die Arithmetik jedes beliebigen (endlichen) Zahlenkörpers aufzubauen. Man beachte, daß der eigentliche Ausgangspunkt der Kummerschen Betrachtung der Gedanke ist, die Gleichung

$$F(x) = 0 \tag{25}$$

n^{ten} Grades, durch welche die den betreffenden Körper erzeugende ganze Zahl bestimmt wird, in bezug auf jede rationale Primzahl p als Kongruenz aufzufassen:

$$F(x) \equiv 0 \quad (\text{mod. } p), \tag{26}$$

und zwischen den Wurzeln der Gleichung und denen der Kongruenz eine eindeutige Zuordnung festzusetzen, welche dann für jede gegebene ganze Zahl des Körpers die idealen Faktoren von p zu definieren gestattet, die in ihr aufgehen. Bei der Durchführung dieses Gedankens für jede beliebig gegebene Gleichung (25) trat nun den Forschern von vornherein ein wesentlicher Unterschied zwischen den besonderen Primzahlen p, welche in der Diskriminante der Gleichung aufgehen,

1) Bachmann, Die Theorie der komplexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind, Berlin 1867; ein Auszug davon im Journ. f. Math. 67, p. 200. Diese Zahlen sind später von Amberg, Inauguraldissertation, Zürich 1897, vom Standpunkte der Idealtheorie aus von neuem untersucht worden. Dirichlets Abhandlung ist die in Nr. 2 zitierte. L. Göring, Inauguraldissertation, Göttingen 1874.

und allen übrigen entgegen; während die Zerlegung der letzteren in ihre idealen Primfaktoren in der Kummerschen Weise in der Tat ohne weitere Schwierigkeiten sich aus der Kongruenz (26) finden ließ, boten jene Diskriminantenteiler wieder besondere Komplikationen dar, die nur durch neue Hilfsmittel überwunden werden konnten. Die erste Arbeit, die über diesen Gegenstand erschienen ist, verdankt man E. Selling.[1]) Indem dieser mit $\varrho_1, \varrho_2, \cdots, \varrho_n$ die Wurzeln der Gleichung (25) bezeichnet, zeigt er, daß ihnen für eine nicht in deren Diskriminante aufgehende Primzahl p diejenigen der Kongruenz (26), die er $r_1, r_2, \cdots, r_n$ nennt, auf verschiedene Weise zugeordnet werden können; irgend eine dieser Zuordnungen sei $r_1^{(i)}, r_2^{(i)}, \cdots, r_n^{(i)}$. Diese Kongruenzwurzeln lassen sich dabei mittels der sogenannten Galoisschen Imaginären, nämlich als Funktionen der Wurzel einer gewissen irreduktibeln Kongruenz (mod. p) ausdrücken. Wird dann eine dem Körper angehörige Zahl, worunter Selling jede ganze rationale Funktion von den Wurzeln der Gleichung versteht, auf eine gewisse Normalform gebracht, in der sie eine ganze Funktion der ϱ_i ist:

$$f(\varrho_1, \varrho_2, \cdots, \varrho_n),$$

und findet dann die Kongruenz

$$f(r_1^{(i)}, r_2^{(i)}, \cdots, r_n^{(i)}) \equiv 0 \quad (\text{mod. } p^m)$$

aber nicht mehr (mod. p^{m+1}) statt, so wird gesagt, die Zahl enthalte den jener Zuordnung entsprechenden idealen Faktor von p genau m Mal. Ist aber p ein Teiler der Diskriminante der Gleichung (25), sodaß die Wurzeln der Kongruenz (26) (mod. p) nicht alle mehr, wie bei den erstbesprochenen Primzahlen, von einander verschieden sind, so muß, um zum Ziele zu gelangen, neben den Wurzeln der irreduktibeln Kongruenz noch eine gewisse Wurzel aus p eingeführt werden, um die r_i

1) E. Selling, Über die idealen Primfaktoren der komplexen Zahlen etc., Ztschr. f. Math. u. Physik, Jhrg. 10, p. 17. Im Anschluß daran s. A. Meyers Abh. „zur Theorie der zerlegbaren Formen, insbesondere der kubischen" Vierteljahrsschrift der Naturf. Ges. zu Zürich, Jhrg. 17, 1897, p. 149.

ausdrücken zu können. Dann hängt die Teilbarkeit der Zahl des Körpers durch einen idealen Faktor von p, wenn λ eine gewisse rationale Zahl bedeutet, von der Potenz von p^λ ab, mit welcher der Ausdruck für

$$f(r_1^{(i)}, r_2^{(i)}, \cdots, r_n^{(i)})$$

beginnt. Die Zahl enthält, wie Selling definiert, den entsprechenden idealen Faktor von p genau m Mal, wenn dieser Ausdruck mit $p^{m\lambda}$ beginnt. Die so definierten idealen Faktoren von p erweisen sich als Primfaktoren und bewirken dann die Zurückführbarkeit der Teilung der betrachteten Gattung von Zahlen auf ganz dieselben Gesetze, wie in den früheren Fällen. Man kann jedoch nicht leugnen, daß diese Sellingsche Theorie außerordentlich schwierig und unübersichtlich, und daß es wünschenswert gewesen ist, sie durch eine andere zu ersetzen. Eine auf ähnlicher Grundlage beruhende Arbeit von Zolotareff[1]) über denselben Gegenstand geht, soviel mir bekannt ist, auf die Ausnahmsfälle, welche die Diskriminantenteiler verursachen können, überhaupt nicht ein.

5. Die genauere Betrachtung der Entwicklungen in Nr. 3 weist nun einen Weg, der eine neue, abweichende Behandlung eines gegebenen Körpers ermöglicht, wie sie in der Tat Dirichlet für einen speziellen biquadratischen Körper in seiner in Nr. 2 zitierten Arbeit durchgeführt hat. Die Theorie der komplexen ganzen Zahlen von der Form $x + y\sqrt{d}$ ist nämlich im Grunde identisch mit der Theorie der binären quadratischen Formen mit der Determinante d. So sahen wir die Frage nach der Zerlegung einer solchen Zahl in ihre einfachsten Faktoren auf die andere nach den Teilern der sogenannten Hauptform $x^2 - dy^2$ zurückgeführt. Ebenso ist die Ermittlung aller Einheiten des betreffenden quadratischen Körpers identisch mit der Auffindung aller ganzzahligen Lösungen der Pellschen Gleichung

$$x^2 - dy^2 = 1,$$

eine Aufgabe, welche bekanntlich zuerst von Lagrange er-

1) Zolotareff, théorie des nombres entiers complexes, avec une application au calcul intégral.

folgreich behandelt und auf die Kettenbruchentwicklung für $\sqrt{d}$ oder, was dasselbe sagt, auf die Reduktion der quadratischen Formen mit der Determinante d zurückgeführt worden ist, während Dirichlet sie aus einer ganz einfachen, fast trivial zu nennenden Tatsache gewann.[1]) Verstehen wir ferner unter p eine ungerade Primzahl, von welcher d quadratischer Rest ist, derart, daß

$$w^2 \equiv d \pmod{p}$$

oder $w^2 - pr = d$ gesetzt werden kann, so folgt aus der den idealen Faktor (p, w) definierenden Kongruenz

$$x + wy \equiv 0 \pmod{p}$$

eine Gleichung

$$x = pz - wy$$

und folglich diese andere

$$x^2 - dy^2 = p\,(pz^2 - 2wzy + ry^2);$$

demnach entspricht dem idealen Faktor (p, w) von p eine quadratische Form (p, w, r) und folglich auch eine ganze Klasse äquivalenter quadratischer Formen mit der Determinante d, durch welche p zur Kongruenzwurzel w gehörig dargestellt werden kann. Dann und nur dann, wenn diese Klasse die Hauptklasse ist, kann p durch die Hauptform $x^2 - dy^2$ dargestellt oder in zwei wirkliche komplexe Faktoren zerlegt werden, dann und nur dann sind also die idealen Primfaktoren (p, w), $(p, -w)$ von p wirklich vorhandene Zahlen des Körpers. Man ersieht hieraus die genaue Bedingung, unter welcher in einem gegebenen quadratischen Körper die Teilbarkeitsgesetze des rationalen Körpers in Gültigkeit bleiben, ohne daß es nötig wäre, ideale Zahlen einzuführen; es geschieht dies so oft, als die Anzahl nicht äquivalenter Klassen quadratischer Formen mit der Determinante d nur Eins ist; im entgegengesetzten Falle bedarf es idealer Zahlen, um die rationalen Primzahlen, welche durch eine der Hauptform nicht äquivalente Form dar-

---

1) S. darüber Dirichlet, Vorles. üb. Zahlentheorie, herausg. von Dedekind, 4. Aufl. § 72—85 und § 141, und vgl. zur ersteren Stelle Bachmann, Vorles. üb. die Natur der Irrationalzahlen. 1892, 4. Vorlesung.

stellbar sind, in ihre wahren Primfaktoren innerhalb des Körpers zu zerlegen. So erweist sich denn überhaupt die Theorie der quadratischen Formen mit der Determinante d als das genaue Korrelat zu derjenigen der komplexen Zahlen von der Gattung $x + y\sqrt{d}$, und Ähnliches gilt ganz allgemein für die Theorie eines beliebigen Zahlenkörpers: immer gibt es eine Gattung aus seinen Zahlen zusammengesetzter, in Linearfaktoren zerlegbarer Formen, deren Theorie der ersteren vollständig entspricht, und man könnte somit versuchen, diese durch jene zu ersetzen und zu ergründen. Wirklich sieht man diesen Weg z. B. von Eisenstein eingeschlagen in seiner oben genannten Arbeit über kubische, der Kreisteilung entstammende Formen. Aber, wollte man auch absehen von den Schwierigkeiten des algebraischen Apparates, welche die Verfolgung dieses Weges behindern, man darf nicht übersehen, daß so der eigentlich arithmetische Kern der Sache: die Eigenschaften der Zahlen des Körpers, verhüllt werden würde. Zwar weist Kronecker mit Recht auf die Wichtigkeit und Bedeutsamkeit der Einführung der quadratischen Formen als „Formen mit zwei Unbestimmten“, wie Gauß sie gefaßt habe, in die reine Arithmetik hin (Festschrift, Journ. f. Math. 92, p. 95), und wie das „methodische Hilfsmittel der Unbestimmten“, das auch für seine eigenen Untersuchungen über algebraische Größen sich ihm so wertvoll erwiesen, in der mehr algebraischen Behandlung der quadratischen Formen dem systematischen Aufbau ihrer Theorie namentlich in deren höheren Teilen zu statten gekommen sei. Dem gegenüber glauben wir aber Dirichlet es als ein besonderes Verdienst zurechnen zu dürfen, daß er bei seinen betreffenden Arbeiten überall, namentlich in seiner Behandlung der Komposition der Formen, die rein arithmetische Bedeutung der Formensätze in helles Licht gesetzt, die Beziehung der Theorie der quadratischen Formen zur Theorie der komplexen Zahlen im Auge behalten, und auch in seinen Untersuchungen über allgemeine zerlegbare Formen das Kapitel, welches man als Lehre von der Transformation dieser Formen in sich selbst zu bezeichnen haben würde, als Theorie der Einheiten des zugehörigen Zahlenkörpers dargestellt hat. Denn das zahlentheoretische Interesse

an der Formentheorie beruht naturgemäß in den arithmetischen Eigenschaften, welche den durch jene Formen darstellbaren Zahlen eben kraft dieser Darstellbarkeit zukommen.

6. Aus solchen Gründen wohl hat Dedekind[1]), der gleichfalls zunächst bemüht gewesen ist, auf dem Kummerschen Wege eine allgemeine, ausnahmslose Theorie der algebraischen Zahlen zu begründen, sich aber darin durch jene schon angedeuteten Ausnahmefälle, welche durch die Teiler der Gleichungsdiskriminante verursacht werden können, behindert sah, nicht zur Theorie der zerlegbaren Formen seine Zuflucht genommen, mit Recht vielmehr diese auf jene zurückgeführt. Ihm verdankt man den ersten Nachweis des Grundes, aus welchem die Kongruenz (26) nicht immer geeignet ist, die Zerlegung der Primzahl p in ihre idealen Primfaktoren in der Kummerschen Weise zu leisten (Näheres darüber s. in Kap. 7); ihm verdankt man aber vornehmlich die Begriffsbildung des Ideals, wie es im vorigen Kapitel von uns eingeführt worden ist und in der Folge die Grundlage der ganzen Theorie bilden wird. Es ist im Grunde nur eine andere Deutung der idealen Zahlen von Kummer. Diese weisen einen zwiefachen Übelstand: einmal ermangeln sie einer allgemeinen, d. i. für jede rationale Primzahl p gleichmäßig geltenden Definition, insofern sie eben nur für jede besondere Primzahl auch durch besondere Kongruenzen festgestellt werden können; sodann bestimmen diese Kongruenzen garnicht sie selbst, sondern nur ihr Vorhandensein als Teiler wirklicher komplexer Zahlen. Erfüllt eine solche komplexe Zahl mehrere derartige Kongruenzen, so ist sie als teilbar anzusehen durch den Komplex der entsprechenden idealen Primfaktoren oder darf teilbar heißen durch deren Produkt, aber auch das Produkt idealer Prim-

---

1) Dedekind gab zuerst seine Theorie in ihren Grundzügen als Anhang zu Dirichlets Vorl. üb. Zahlentheorie, 2. Auflage, dann eine sehr instruktive Darstellung derselben im Bull. des sc. math. et astron. 1. série 11 und 2. série 1, welche auch besonders erschienen ist Paris, Gauthier-Villars 1877; sehr vermehrt findet sie sich in der 3. Auflage und zum Teil wesentlich umgearbeitet in der 4. Auflage des erstgenannten Werkes.

faktoren ist, wie schon bemerkt, im allgemeinen bloß wieder eine ideale Zahl, die nicht an sich darstellbar, sondern nur als Teiler durch jene Kongruenzen definiert ist, und nur, wenn durch die letztere die Teilbarkeit einer komplexen Zahl erschöpft ist, ist jene ideale Zahl als mit dieser identisch zu betrachten. Aber, ohne die Kummersche Grundlage zu verlassen, kann die ideale Zahl durch eine andere Bildung ersetzt werden, die immer real und daher für sich angebbar ist, und so lassen sich die besagten Übelstände vermeiden.

Ist nämlich etwa ein idealer Primfaktor von p definiert durch die Kongruenz

$$x + wy \equiv 0 \pmod{p}, \tag{27}$$

so findet man daraus die Gesamtheit aller komplexen ganzen Zahlen der Gattung $x + y\sqrt{d}$, in welchen der ideale Primfaktor aufgeht, indem man die ganzen Zahlen x, y der Kongruenz (27) gemäß wählt, derzufolge, unter z irgend eine ganze Zahl verstanden,

$$x = pz - wy$$

gesetzt werden darf. Die Gesamtheit der durch jenen idealen Primfaktor aufgehenden komplexen Zahlen ist also diejenige der Zahlen

$$pz + (\sqrt{d} - w)y$$

oder der Modulus

$$\pi = [p, \sqrt{d} - w], \tag{28}$$

da auch umgekehrt einleuchtet, daß jede in diesem enthaltene Zahl $x + y\sqrt{d}$ der Kongruenz (27) genügt. Wie nun eine rationale ganze Zahl m eindeutig definiert ist durch die Gesamtheit aller ihrer Vielfachen, in gleicher Weise darf man den Modulus (28), d. i. die Gesamtheit aller durch den gedachten idealen Primfaktor teilbaren komplexen ganzen Zahlen der Gattung zur Definition des letztern benutzen oder ihm als gleichbedeutend substituieren. Dem Modulus π kommt zufolge der Identität

$$\left(pz + (\sqrt{d} - w)y\right) \cdot (x' + y'\sqrt{d})$$
$$= p(zx' - ryy' + wzy') + (\sqrt{d} - w) \cdot (yx' + pzy' - wyy'),$$

in welcher $w^2 - d = pr$ gedacht ist, die charakteristische Eigen-

schaft zu, daß jede seiner Zahlen mit einer beliebigen komplexen ganzen Zahl des Körpers multipliziert, wieder eine Zahl des Modulus gibt. Der Definition in Nr. 4 des vorigen Kapitels gemäß ist er also ein Ideal des aus $\sqrt{d}$ gebildeten quadratischen Körpers. So sehen wir die nur ausnahmsweise an sich existierenden idealen Zahlen Kummers durch das stets völlig reale Dedekindsche Gebilde des Ideals, d. i. eines bestimmten Komplexes von unendlich vielen wirklichen Zahlen des Körpers aufs einfachste und anschaulichste ersetzt. Wie dieser Begriff sich dazu eignet, zu leisten, was Dedekind erstrebt hat, nämlich die allgemeine Arithmetik eines jeden Zahlenkörpers fest zu begründen und auf die einfachen Gesetze des rationalen Zahlenkörpers zurückzuführen, das zu zeigen wird die Aufgabe der nachfolgenden Abschnitte sein. Hier, wo es sich nur darum handelte, die geschichtliche Entwicklung der Theorie und die Entstehung des Idealbegriffs zu skizzieren, bedarf es nicht noch weiterer Auseinandersetzungen bezüglich des vorliegenden besonderen Zahlenkörpers, dessen Arithmetik vielmehr in einem späteren Teile unsers Werks darzustellen beabsichtigt wird.

Auf einem verwandten, aber in der Fassung wesentlich verschiedenen Grundbegriffe beruht die Kroneckersche Theorie der algebraischen Größen, und diese verschiedene Fassung eben auf dem Umstande, daß Kronecker die Theorie der algebraischen Größen im Auge hat, von denen die algebraischen Zahlen nur einen ganz besonderen Fall ausmachen. Unter einer algebraischen Größe ist jede Wurzel einer algebraischen Gleichung zu verstehen, deren Koeffizienten einem aus algebraischen Zahlen und beliebig viel Unbestimmten $u_1, u_2, u_3, \cdots$ gebildeten Rationalitätsbereich angehören. Die natürliche Grundlage ihrer Theorie bildet nach Kronecker die Betrachtung der Formen, d. i. der ganzen Funktionen dieser Unbestimmten mit rationalen und allgemeiner mit algebraischen Koeffizienten. So treten die Unbestimmten auch in jenen Kroneckerschen Grundbegriff ein, auf welchem er seine Theorie der Formen und die Gesetze ihrer Teilbarkeit erbaut, den Begriff des algebraischen Divisors. Sind nämlich $\alpha, \alpha_1, \alpha_2, \cdots$ irgend welche ganzen Zahlen eines Körpers, so kann nach Kronecker

ihr größter gemeinsamer Teiler durch den Ausdruck

$$\frac{\alpha + \alpha_1 u_1 + \alpha_2 u_2 + \cdots}{Fm(\alpha + \alpha_1 u_1 + \alpha_2 u_2 + \cdots)},$$

dessen Nenner die ganze ganzzahlige Funktion ist, welche aus der Norm

$$Nm(\alpha + \alpha_1 u_1 + \alpha_2 u_2 + \cdots)$$

durch Unterdrückung des größten gemeinsamen Teilers ihrer ganzzahligen Koeffizienten hervorgeht, dargestellt werden, da jede lineare Funktion

$$\alpha + \alpha_1 v_1 + \alpha_2 v_2 + \cdots$$

jener Zahlen durch den gedachten Ausdruck teilbar, der Quotient dann aber durch keinen ähnlichen Ausdruck mehr teilbar ist. Sieht man von dem Nenner des Divisors ab, der in der Theorie die Rolle einer Einheit spielt, so ist jener im wesentlichen mit der Linearform

$$\alpha u + \alpha_1 u_1 + \alpha_2 u_2 + \cdots,$$

aus welcher die Zahlen des Körperideales

$$\{\alpha, \alpha_1, \alpha_2, \cdots\}$$

entstehen, wenn die Unbestimmten $u, u_1, u_2, \cdots$ alle ganzen Zahlen des Körpers durchlaufen, identisch. Indem Kronecker an die Stelle dieses Ideales seinen Divisor treten läßt, erreicht er den an sich gewiß nicht zu unterschätzenden Vorteil, „den gemeinsamen Teiler algebraischer Zahlen aus der Sphäre bloßer Abstraktion in die Wirklichkeit algebraischer Gebilde zu versetzen“, an denen dann in konkreter Weise „die bei den Idealen benutzten abstrakten Eigenschaften sich vereinigen“, aber im Ideale tritt mehr die „Richtung auf das Innerliche“ hervor, welche der Mathematik schon von Gauß, vornehmlich aber von Dirichlet und Riemann gegeben worden ist, nach der es sich empfiehlt, die mathematischen Wahrheiten „ex notionibus potius quam ex notationibus“, nicht so sehr mittels formaler Betrachtungen, als unmittelbar aus den charakteristischen Begriffen zu entwickeln.[1]) Seine Theorie steht so zu

1) S. Dedekind üb. die Begründung der Idealtheorie, Götting. Nachr. 1895, sowie sur la théorie des nombres entiers algébriques, Paris, Gauthier-Villars, 1877, p. 59.

derjenigen Dedekinds in einigermaßen ähnlichem Verhältnisse, wie die Theorie der Funktionen von Weierstraß zu derjenigen von Riemann. Näher auf sie und dieses Verhältnis hier einzugehen, verbietet uns der Plan unsers Werkes.

Sechstes Kapitel.

Die Arithmetik der Körperideale.

1. Nachdem wir im vorigen Kapitel an einem Beispiele die Entstehung des Idealbegriffs erläutert haben, kehren wir zur allgemeinen Betrachtung wieder zurück, um jetzt mittels desselben die Gesetze für die Teilbarkeit der Zahlen eines beliebigen Körpers $K(\mathsf{A};\,R)$ n^{ten} Grades zu entwickeln.

Wir beginnen diese Untersuchung mit der allgemeinen Bemerkung, daß jedes Ideal nach seiner Definition ein Modulus von der Art ist, wie sie im zweiten Kapitel betrachtet worden sind, und daß somit die dort hergeleiteten Sätze insbesondere auch für Ideale ihre Gültigkeit behalten. Aber Ideale sind zugleich Moduln von einem ausgezeichneten Charakter, denn für jedes Ideal besteht die Beziehung

$$\mathfrak{g}\mathfrak{j} = \mathfrak{j}. \tag{1}$$

Wesentlich dieser besonderen Eigenschaft der Ideale ist es zu verdanken, daß sich für sie eine Arithmetik aufstellen läßt, welche der Arithmetik gewöhnlicher Zahlen völlig konform ist.

Sind zwei Ideale $\mathfrak{j}, \mathfrak{j}'$ gegeben, so sind nach der Theorie der Moduln zugleich auch die folgenden Moduln bestimmt:

$$\mathfrak{j}+\mathfrak{j}',\quad \mathfrak{j}-\mathfrak{j}',\quad \mathfrak{j}\cdot\mathfrak{j}',$$

die wir resp. als größten gemeinsamen Teiler, kleinstes gemeinsames Vielfache und Produkt der Moduln $\mathfrak{j}, \mathfrak{j}'$ bezeichneten; diese aber sind Ideale. Denn, sie sind erstens Moduln in $\mathfrak{g}$. Ferner aber besteht $\mathfrak{j}+\mathfrak{j}'$ aus den Zahlen $i+i'$, von denen die erste in $\mathfrak{j}$, die zweite in $\mathfrak{j}'$ enthalten ist; dann sind aber, welche ganze Zahl des Körpers auch unter γ verstanden

werde, die Zahlen γi, $\gamma i'$ wieder Zahlen in $\mathfrak{j}$, $\mathfrak{j}'$ resp., also $\gamma(i + i')$ eine Zahl in $\mathfrak{j} + \mathfrak{j}'$, d. h. die für ein Ideal charakteristischen Beziehungen (22) des vierten Kapitels sind für den Modulus $\mathfrak{j} + \mathfrak{j}'$ erfüllt:

$$\mathfrak{j} + \mathfrak{j}' \succ \mathfrak{g}, \quad \mathfrak{g}(\mathfrak{j} + \mathfrak{j}') \succ \mathfrak{j} + \mathfrak{j}'.$$

Ist jetzt i eine Zahl, welche sowohl in $\mathfrak{j}$ als in $\mathfrak{j}'$ enthalten ist, so gilt das Gleiche von γi, mithin ist

$$\mathfrak{j} - \mathfrak{j}' \succ \mathfrak{g}, \quad \mathfrak{g}(\mathfrak{j} - \mathfrak{j}') \succ \mathfrak{j} - \mathfrak{j}'.$$

Endlich ist wegen (1)

$$\mathfrak{j} \cdot \mathfrak{j}' = \mathfrak{g}\mathfrak{j} \cdot \mathfrak{j}' = \mathfrak{g} \cdot \mathfrak{j}\mathfrak{j}'$$

und somit auch $\mathfrak{j}\mathfrak{j}'$ ein Ideal.

Richten wir nun vorerst unsere Aufmerksamkeit auf das Produkt

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b}$$

zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$. Wir könnten die letzteren mit Hurwitz „Teiler" des Produkts $\mathfrak{c}$ nennen, wenn wir nicht bereits mit diesem Ausdrucke ein anderes Verhältnis bezeichnet hätten, von welchem von vornherein durchaus nicht einleuchtet, ob es mit dem Umstande, daß das Produkt durch Multiplikation der beiden Ideale entsteht, identisch sei oder nicht: wir haben nach Dedekind $\mathfrak{c}$ teilbar durch $\mathfrak{a}$ oder $\mathfrak{a}$ einen Teiler von $\mathfrak{c}$ genannt, wenn die Beziehung

$$\mathfrak{c} \succ \mathfrak{a} \tag{2}$$

erfüllt, nämlich $\mathfrak{c}$ in $\mathfrak{a}$ enthalten ist. Daher wollen wir einstweilen die im Produkte $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ auftretenden Ideale $\mathfrak{a}$, $\mathfrak{b}$ die Faktoren des Produkts nennen. Es wird nun den Kernpunkt unserer nächsten Untersuchungen ausmachen, das Verhältnis festzustellen, welches zwischen der Multiplikation und der Teilbarkeit der Ideale stattfindet, das Verhältnis nämlich zwischen der Beziehung (2) und der anderen Beziehung

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b}, \tag{3}$$

wenn in dieser mit $\mathfrak{a}$ und $\mathfrak{c}$ zugleich auch $\mathfrak{b}$ ein Ideal sein soll, indem wir nachweisen, daß die letztere Beziehung oder der Ausspruch „$\mathfrak{a}$ sei ein Faktor von $\mathfrak{c}$", völlig

gleichbedeutend ist mit dem anderen „$\mathfrak{c}$ sei enthalten in $\mathfrak{a}$“ oder teilbar durch $\mathfrak{a}$, was die Formel (2) zum Ausdrucke bringt.

Es leuchtet nun zwar in dieser Hinsicht ohne weiteres ein, daß, wenn eine Beziehung (3) stattfindet, das Ideal $\mathfrak{c}$ in jedem der Ideale $\mathfrak{a}$, $\mathfrak{b}$ enthalten sein muß, mit anderen Worten: aus (3) folgt jede der beiden Beziehungen

$$(4) \qquad \mathfrak{c} \succ \mathfrak{a}, \quad \mathfrak{c} \succ \mathfrak{b}.$$

Denn, bedeuten α, β die in $\mathfrak{a}$, $\mathfrak{b}$ resp. also auch in $\mathfrak{g}$ enthaltenen Zahlen, so besteht $\mathfrak{c}$ aus den Produkten $\alpha \cdot \beta$ und beliebigen Summen solcher Produkte, deren jedes, der Definition eines Ideales zufolge, sowohl zu $\mathfrak{a}$ als auch zu $\mathfrak{b}$ gehört, daher sind die sämtlichen Zahlen von $\mathfrak{c}$ in jedem dieser beiden Ideale enthalten, so daß man die Beziehungen (4) und genauer noch die folgende

$$(5) \qquad \mathfrak{c} \succ \mathfrak{a} - \mathfrak{b}$$

aussagen darf. Jeder Faktor eines Ideales ist also auch (im Dedekindschen Sinne) ein Teiler desselben. Zur Begründung des vorher ausgesprochenen Äquivalenzsatzes würde aber die Umkehrbarkeit dieses Resultates erforderlich sein, daß nämlich auch umgekehrt aus dem Stattfinden der Beziehung (2) die Existenz eines Ideales $\mathfrak{b}$ folgt, für welches $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ gesetzt werden kann.

2. Bevor wir der Erledigung dieses Hauptpunktes der Theorie uns zuwenden, nähern wir uns ihr durch die Betrachtung einfacherer Verhältnisse, indem wir zunächst uns auf Hauptideale beschränken. Sind $\mathfrak{g}\alpha$, $\mathfrak{g}\beta$, $\mathfrak{g}\gamma$ drei solche Ideale, zwischen denen die Gleichung

$$(6) \qquad \mathfrak{g}\gamma = \mathfrak{g}\alpha \cdot \mathfrak{g}\beta$$

besteht, so folgen nach dem eben Bewiesenen die beiden Beziehungen

$$(7) \qquad \mathfrak{g}\gamma \succ \mathfrak{g}\alpha, \quad \mathfrak{g}\gamma \succ \mathfrak{g}\beta.$$

Ihnen zufolge ist insbesondere die Zahl γ sowohl in $\mathfrak{g}\alpha$ als in $\mathfrak{g}\beta$ enthalten, d. i. sowohl durch α als auch durch β, ja wegen (6) sogar durch $\alpha \cdot \beta$ teilbar; da aber umgekehrt $\alpha \cdot \beta$ eine im Produkte zur Rechten von (6) vorhandene Zahl, also

wegen der linken Seite durch γ teilbar ist, so sind γ und $\alpha\beta$ einander gleich oder assoziiert; aus (6) folgt mithin wenigstens bis auf einen, einer Einheit gleichen Faktor die Gleichheit

$$\gamma = \alpha\beta. \tag{8}$$

Hier erkennt man aber unmittelbar die Umkehrbarkeit des Resultates. Denn, besteht die Beziehung

$$\mathfrak{g}\gamma \succ \mathfrak{g}\alpha, \tag{9}$$

ist also insonderheit γ teilbar durch α, sodaß $\gamma = \alpha\beta$ gesetzt werden kann, während auch β eine Zahl in $\mathfrak{g}$ ist, so wird zunächst

$$\mathfrak{g}\gamma = \mathfrak{g} \cdot \alpha\beta \tag{10}$$

sein. Nun besteht aber das Produkt $\mathfrak{g}\alpha \cdot \mathfrak{g}\beta$ aus allen Zahlen von der Form $\gamma\gamma' \cdot \alpha\beta$, wo γ, γ' also auch $\gamma\gamma'$ Zahlen in $\mathfrak{g}$ sind, und aus beliebigen Summen solcher Produkte; aus der Gleichheit $\mathfrak{g}\mathfrak{g} = \mathfrak{g}$ geht jedoch hervor, daß auch jede Zahl in $\mathfrak{g}$ als ein Produkt von der Art $\gamma\gamma'$ oder als eine Summe solcher Produkte aufgefaßt werden kann, und somit ist die Gesamtheit der vorgedachten Zahlen nichts anderes als $\mathfrak{g} \cdot \alpha\beta$. Demnach darf man die Gleichung (10) auch schreiben wie folgt:

$$\mathfrak{g}\gamma = \mathfrak{g}\alpha \cdot \mathfrak{g}\beta \tag{11}$$

und aus der Formel (9) fließt mithin auch die Gleichung (6)

Man erkennt hieraus, daß für Hauptideale $\mathfrak{a}, \mathfrak{c}$ die Beziehung (2) völlig gleichbedeutend ist mit dem Stattfinden einer Gleichung (3), in welcher auch der Faktor $\mathfrak{b}$ ein Hauptideal ist, oder daß bei der Beschränkung auf Hauptideale der Begriff des Teilers mit demjenigen eines Faktors sich deckt. Ferner sind die beiden Gleichungen (6) und (8) einander äquivalent, d. h. die Teilbarkeit einer Zahl γ durch eine Zahl α ist gleichbedeutend mit der Teilbarkeit des Ideals $\mathfrak{g}\gamma$ durch das Ideal $\mathfrak{g}\alpha$. Die Gesetze für die Teilbarkeit der Zahlen eines Körpers $K(\mathsf{A}; R)$ sind demnach vollständig in denjenigen enthalten, welche für die Teilbarkeit seiner Ideale Geltung haben, und werden mit den letzteren identisch sein, sooft im Körper überhaupt nur Hauptideale vorhanden sind.

Aus der Gleichheit

$$\mathfrak{g}\alpha = \mathfrak{g}\beta$$

zweier Hauptideale folgt auch, wenigstens bis auf einen Einheitsfaktor die Gleichheit

$$\alpha = \beta$$

der Zahlen; denn die im ersten Ideale enthaltene Zahl α muß, weil auch im zweiten enthalten, durch β und ebenso β durch α teilbar und deshalb α, β, wenn nicht gleich, doch einander assoziiert sein.

Für zwei beliebige Hauptideale $\mathfrak{g}\alpha, \mathfrak{g}\beta$ aber besteht die Gleichheit

$$\beta \cdot \mathfrak{g}\alpha = \alpha \cdot \mathfrak{g}\beta, \tag{12}$$

welche dem kurz zuvor Bemerkten zufolge auch in der Form

$$\mathfrak{g}\beta \cdot \mathfrak{g}\alpha = \mathfrak{g}\alpha \cdot \mathfrak{g}\beta$$

geschrieben werden kann und nur die Kommutativität der Multiplikation von Moduln für den vorliegenden Fall zum Ausdrucke bringt. Hiernach gibt es bei je zwei Hauptidealen Zahlen in $\mathfrak{g}$, durch welche multipliziert sie einander gleich werden. Derartige Multiplikatoren, für welche also

$$\alpha' \cdot \mathfrak{j} = \alpha \cdot \mathfrak{j}' \tag{13}$$

würde, gibt es bei irgend zwei gegebenen Idealen $\mathfrak{j}, \mathfrak{j}'$ im allgemeinen nicht, vielmehr drückt das Vorhandensein zweier ganzer Zahlen α, α' des Körpers, welche diese Gleichung erfüllen, eine ausgezeichnete Beziehung zwischen den beiden Idealen aus, kraft deren wir sie einander *äquivalent* nennen wollen. Aus dieser Definition der Äquivalenz von Idealen geht dann sogleich hervor, daß zwei Ideale, welche ein- und demselben Ideale äquivalent sind, es auch unter einander sein müssen. Denn aus den Gleichungen

$$\alpha'\mathfrak{j} = \alpha\mathfrak{j}', \quad \beta''\mathfrak{j} = \beta\mathfrak{j}'',$$

wo $\mathfrak{j}, \mathfrak{j}', \mathfrak{j}''$ drei Ideale, $\alpha, \alpha', \beta, \beta''$ Zahlen in $\mathfrak{g}$ bedeuten, folgt sogleich die andere:

$$\alpha\beta'' \cdot \mathfrak{j}' = \beta\alpha' \cdot \mathfrak{j}'',$$

welche die Aussage bestätigt. Sonach lassen sich nun alle Ideale des Körpers in Klassen verteilen, indem man immer alle ein- und demselben Ideale äquivalenten Ideale in eine Klasse zusammenfaßt; die unter einander äquivalenten

Ideale gehören dann der gleichen Klasse, zwei nicht äquivalente Ideale aber stets verschiedenen Klassen an. Hier fragt es sich sogleich, ob die Anzahl dieser Klassen endlich sei, und bejahenden Falles, wie groß? Sehr bald werden wir zeigen, daß in der Tat die erste Frage zu bejahen ist; die Bestimmung der Anzahl der Klassen selbst jedoch läßt sich bisher nur mittels Betrachtungen ausführen, welche den von Dirichlet zur Ermittelung der Klassenanzahl quadratischer Formen erfundenen analytischen Methoden nachgebildet sind, und kann erst später mitgeteilt werden.

Alle Hauptideale sind, wie aus (12) hervorgeht, unter einander äquivalent, gehören mithin nur einer einzigen Klasse an, welche die Hauptklasse H genannt werden soll; umgekehrt enthält aber diese Klasse auch nur Hauptideale. Denn, ist ein Ideal $\mathfrak{j}$ einem Hauptideale $\mathfrak{g}\alpha$ äquivalent, sodaß Zahlen β, γ in $\mathfrak{g}$ vorhanden sind, für welche

$$\mathfrak{j} \cdot \gamma = \mathfrak{g}\alpha \cdot \beta$$

ist, so muß die in dem Ideale zur Rechten enthaltene Zahl $\alpha\beta$, weil auch in demjenigen zur Linken enthalten, durch γ teilbar, also $\alpha\beta = \gamma\delta$ sein, wo auch δ eine Zahl in $\mathfrak{g}$ bedeutet; dadurch nimmt die vorige Gleichung die Form an:

$$\mathfrak{j} \cdot \gamma = \mathfrak{g}\delta \cdot \gamma$$

und ergibt offenbar die Gleichheit $\mathfrak{j} = \mathfrak{g}\delta$.

Jede Klasse ist durch irgend ein in ihr befindliches Ideal $\mathfrak{j}$ unzweideutig bestimmt, denn alle ihre Ideale ergeben sich nach der die Äquivalenz definierenden Gleichung (13) aus $\mathfrak{j}$ durch Multiplikation mit dem Quotienten gewisser Zahlen in $\mathfrak{g}$. Das beliebig aus der Klasse herausgegriffene Ideal $\mathfrak{j}$ kann daher als Repräsentant derselben aufgefaßt werden. Sind nun $\mathfrak{a}$, $\mathfrak{b}$ Repräsentanten zweier Idealklassen A, B, so ist auch das Produkt $\mathfrak{a}\mathfrak{b}$ ein Ideal und gehört also einer ganz bestimmten Idealklasse C an. Letztere aber ist völlig unabhängig von der willkürlichen Wahl der Repräsentanten von A, B, also nur durch diese Klassen selbst bestimmt. In der Tat, sind $\mathfrak{a}'$, $\mathfrak{b}'$ zwei beliebige andere zu den Klassen A, B resp. gehörige Ideale, derart, daß Gleichungen bestehen von der Form

$$\alpha'\mathfrak{a} = \alpha\mathfrak{a}', \ \beta'\mathfrak{b} = \beta\mathfrak{b}'$$

mit den in $\mathfrak{g}$ vorhandenen Zahlen $\alpha, \alpha', \beta, \beta'$, so folgt sogleich

$$\alpha'\beta' \cdot \mathfrak{a}\mathfrak{b} = \alpha\beta \cdot \mathfrak{a}'\mathfrak{b}',$$

d. h. $\mathfrak{a}'\mathfrak{b}'$ gehört derselben Klasse an, wie $\mathfrak{a}\mathfrak{b}$. Die solcherweise durch die beiden Klassen A, B völlig bestimmte Klasse C soll aus A, B zusammengesetzt oder das Produkt dieser Klassen genannt und dies durch die Gleichung

$$C = AB = BA \tag{14}$$

ausgedrückt werden. Durch Zusammensetzung einer Klasse mit der Hauptklasse bleibt jene ungeändert, mit anderen Worten: es ist stets

$$AH = HA = A; \tag{15}$$

in der Tat kann H durch das Ideal $\mathfrak{g}$ repräsentiert werden, für welches die Gleichheit $\mathfrak{g}\mathfrak{a} = \mathfrak{a}$ also auch die Äquivalenz beider Ideale besteht.

Weitere Sätze über Idealklassen werden wir den erhaltenen noch hinzufügen können, sobald wir die Endlichkeit ihrer Anzahl werden festgestellt haben. Jetzt aber zur Kernfrage der vorigen Nummer uns zurückwendend, beschließen wir die vorläufigen Betrachtungen mit zwei einfachen Bemerkungen.

1) Das Ideal $\mathfrak{g}$ ist das einzige, welches die Zahl 1 in sich enthält. Da in einem Ideale $\mathfrak{j}$ mit der Zahl 1 zugleich auch der Modulus $\mathfrak{z}$ enthalten sein muß und umgekehrt, so kommt dieser Ausspruch auf den anderen hinaus, daß $\mathfrak{g}$ das einzige Ideal $\mathfrak{j}$ sei, für welches

$$\mathfrak{z} \succ \mathfrak{j}$$

ist. Daß diese Beziehung für $\mathfrak{j} = \mathfrak{g}$ besteht, zeigt Gleichung (9) des 4. Kapitels; wenn sie aber besteht, so gehört die Zahl 1, also der Definition eines Ideales zufolge auch jede Zahl $1 \cdot \gamma$, nämlich jede Zahl in $\mathfrak{g}$ dem Ideale $\mathfrak{j}$ an, dessen Zahlen doch auch umgekehrt zu $\mathfrak{g}$ gehören, also ist $\mathfrak{j} = \mathfrak{g}$.

2) Stellt man sich die allgemeinere Frage für irgend eine (positive) ganze rationale Zahl a, so lautet die Antwort: daß eine solche nur in einer endlichen Anzahl von Idealen vorhanden sein kann. Sei nämlich

$\mathfrak{j}$ ein Ideal, welches die Zahl a enthält; denkt man sich dasselbe als n-gliedrigen Modulus:

$$\mathfrak{j} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$$

und seine Basiszahlen α_i als Zahlen in $\mathfrak{g}$ dargestellt in der Form

$$\alpha_i = g_{i1}\gamma_1 + g_{i2}\gamma_2 + \cdots + g_{in}\gamma_n, \quad (i = 1, 2, \cdots, n)$$

so erhält man, da $g_{ik} = a \cdot q_{ik} + r_{ik}$ gesetzt und hierbei r_{ik} nicht negativ und kleiner als a gedacht werden kann, die Gleichung

$$(16) \qquad \alpha_i = a \cdot \gamma^{(i)} + \alpha_i',$$

während

$$(17) \quad \gamma^{(i)} = q_{i1}\gamma_1 + q_{i2}\gamma_2 + \cdots + q_{in}\gamma_n, \quad \alpha_i' = r_{i1}\gamma_1 + r_{i2}\gamma_2 + \cdots + r_{in}\gamma_n$$

ist; diesen Gleichungen zufolge ist jede der Zahlen α_i' als Differenz $\alpha_i - a\gamma^{(i)}$ zweier in $\mathfrak{j}$ enthaltenen Zahlen selbst eine Zahl in $\mathfrak{j}$. Hieraus folgt ferner, wenn die u_i ganze Zahlen bedeuten,

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$
$$= a \cdot \gamma + (\alpha_1' u_1 + \alpha_2' u_2 + \cdots + \alpha_n' u_n),$$

unter γ eine gewisse Zahl in $\mathfrak{g}$ verstanden, und nach dieser Gleichung ist jede Zahl in $\mathfrak{j}$ eine Zahl des Modulus

$$\mathfrak{g}a + [\alpha_1', \alpha_2', \cdots, \alpha_n'];$$

da aber sowohl a (und also auch jede Zahl in $\mathfrak{g}a$), als auch jede Zahl des Modulus $[\alpha_1', \alpha_2', \cdots, \alpha_n']$ im Ideale $\mathfrak{j}$ enthalten ist, so gilt dasselbe auch von dem vorstehenden Modulus und somit ist

$$(18) \qquad \mathfrak{j} = \mathfrak{g}a + [\alpha_1', \alpha_2', \cdots, \alpha_n'].$$

Nun gibt es wegen der den Zahlen r_{ik} im Ausdrucke (17) für α_i' auferlegten Beschränkung nur eine endliche Anzahl von Werten für jede der Zahlen α_i', also auch nur eine endliche Anzahl von Moduln $[\alpha_1', \alpha_2', \cdots, \alpha_n']$. Da aber für jedes Ideal, in welchem die Zahl a enthalten ist, eine Gleichung von der Form (18) stattfindet, so kann auch die Anzahl derartiger Ideale nur eine endliche sein.

Hieraus folgt leicht weiter der Satz: Jedes Ideal ist nur durch eine endliche Anzahl von Idealen teilbar, das soll sagen: in einer endlichen Anzahl anderer Ideale enthalten. In der Tat, sei α eine beliebige, von Null verschiedene Zahl des Ideals $\mathfrak{j}$, welches daher auch die Norm $N(\alpha)$ und deren Absolutwert a, der eine positive ganze rationale Zahl ist, enthält. Ist dann das Ideal $\mathfrak{j}$ also auch die Zahl a in einem Ideale $\mathfrak{j}'$ enthalten, so kann sich $\mathfrak{j}'$ nur unter der endlichen Anzahl derjenigen Ideale befinden, welche a enthalten, also selbst nur in endlicher Anzahl vorhanden sein.

3. Nunmehr handele es sich um den *Nachweis* des Satzes, daß, wenn für zwei Ideale $\mathfrak{a}$, $\mathfrak{c}$ die Beziehung besteht

$$\mathfrak{c} \succ \mathfrak{a}, \tag{19}$$

das Ideal $\mathfrak{c}$ als Produkt zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$ aufgefaßt werden kann. Diesem Ausspruche ist aber der andere vollkommen gleichbedeutend: daß für jedes Ideal $\mathfrak{j}$ ein anderes Ideal $\mathfrak{j}'$ angebbar ist, von der Beschaffenheit, daß $\mathfrak{j} \cdot \mathfrak{j}'$ ein Hauptideal sei. In der Tat folgert man zunächst den zweiten Satz aus dem ersten, denn, wenn dieser gilt, so wird, da das irgend einer in $\mathfrak{j}$ enthaltenen Zahl α entsprechende Ideal $\mathfrak{g}\alpha$ ebenfalls in $\mathfrak{j}$ enthalten sein muß, ein Ideal $\mathfrak{j}'$ vorhanden sein der Art, daß $\mathfrak{g}\alpha = \mathfrak{j} \cdot \mathfrak{j}'$ ist. Umgekehrt folgt aber auch der erste Satz aus dem zweiten, denn, wenn die Beziehung (19) stattfindet, so ist auch

$$\mathfrak{c}\mathfrak{m} \succ \mathfrak{a}\mathfrak{m}$$

für jedes Ideal $\mathfrak{m}$; kann dies also, wie der zweite Satz behauptet, so gewählt werden, daß $\mathfrak{a} \cdot \mathfrak{m}$ ein Hauptideal $\mathfrak{g}\alpha$ wird, so ist auch

$$\mathfrak{c}\mathfrak{m} \succ \mathfrak{g}\alpha$$

d. h. alle Zahlen des Ideals $\mathfrak{c}\mathfrak{m}$ sind von der Form $\gamma\alpha$, wo γ eine Zahl in $\mathfrak{g}$, und die Gesamtheit $\mathfrak{b}$ dieser Zahlen γ, welche den Zahlen in $\mathfrak{c}\mathfrak{m}$ entsprechen, bildet ersichtlich nicht nur einen Modulus, sondern auch ein Ideal, da, wenn $\gamma^{(0)}$ irgend eine Zahl in $\mathfrak{g}$ ist, auch $\gamma^{(0)} \cdot \gamma\alpha = \gamma^{(0)}\gamma \cdot \alpha$ eine Zahl in $\mathfrak{c}\mathfrak{m}$, mithin $\gamma^{(0)} \cdot \gamma$ eine Zahl in $\mathfrak{b}$ ist. Hiernach ist

$$\mathfrak{c}\mathfrak{m} = \mathfrak{b} \cdot \alpha,$$

aus welcher Gleichung durch Multiplikation mit $\mathfrak{a}$ und Berücksichtigung der Gleichheit $\mathfrak{a}\mathfrak{m} = \mathfrak{g}\alpha$ die folgende:

$$\mathfrak{c} \cdot \alpha = \mathfrak{a}\mathfrak{b} \cdot \alpha$$

und aus dieser auch

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b}$$

hervorgeht. — Wir dürfen daher, statt den Beweis des ersten Satzes zu suchen, unsere Bemühung darauf richten, einen Beweis des zweiten zu finden.

Es ist nun hochinteressant, wie eng dieser letztere, fundamentale Satz der Arithmetik der algebraischen Zahlen mit jenem in den Disquisitiones arithmeticae Art. 42 zuerst von *Gauss* gegebenen Fundamentalsatze über die Zerlegbarkeit ganzer Funktionen einer Veränderlichen verbunden ist.

Dieser Satz lautet wie folgt: Sind

$$(20)\qquad \begin{aligned} A(x) &= x^m + a_1 x^{m-1} + \cdots + a_m \\ B(x) &= x^n + b_1 x^{n-1} + \cdots + b_n \end{aligned}$$

zwei ganze Funktionen von x, deren höchste Koeffizienten gleich 1, die übrigen rationale, doch nicht sämtlich *ganze* Zahlen sind, so sind auch die Koeffizienten des Produktes

$$(21)\qquad C(x) = x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n}$$

nicht sämtlich rationale *ganze* Zahlen. Da jedenfalls die Koeffizienten c_i rational sein werden, setze man, mit γ_0 ihren Generalnenner bezeichnend, allgemein $c_i = \frac{\gamma_i}{\gamma_0}$ und ebenso $a_i = \frac{\alpha_i}{\alpha_0}$, $b_i = \frac{\beta_i}{\beta_0}$, wo α_0, β_0 die Generalnenner der a_i bez. w. der b_i bezeichnen. Dadurch erhält man folgende Gleichheit:

$$(22)\qquad \alpha_0\beta_0 \cdot C'(x) = \gamma_0 \cdot A'(x)\, B'(x),$$

worin

$$(23)\qquad \begin{cases} A'(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m \\ B'(x) = \beta_0 x^n + \beta_1 x^{n-1} + \cdots + \beta_n \\ C'(x) = \gamma_0 x^{m+n} + \gamma_1 x^{m+n-1} + \cdots + \gamma_{m+n} \end{cases}$$

gedacht sind; in jeder der so definierten Funktionen $A'(x)$, $B'(x)$, $C'(x)$ werden, der Natur des Generalnenners gemäß, die Koeffizienten ganze Zahlen ohne gemeinsamen Teiler sein, und

wegen solcher Eigenschaft mögen die Funktionen ursprüngliche oder primitive Funktionen heißen. Sind nun, wie der Satz voraussetzt, die Koeffizienten a_i, b_i nicht sämtlich ganze Zahlen, so muß $\alpha_0\beta_0$ von 1 verschieden sein, mithin mindestens einen Primfaktor haben; ein beliebiger von diesen sei p. Da durch ihn weder sämtliche α_i, noch sämtliche β_i aufgehen können, so gibt es in der Reihe der ersteren einen ersten Koeffizienten α_h, in der Reihe der zweiten einen ersten Koeffizienten β_k, der nicht durch p teilbar ist, und dann wird der Koeffizient von $x^{m+n-h-k}$ im Produkte $A'(x)\,B'(x)$, nämlich die Summe

$$\cdots \alpha_{h+1}\beta_{k-1} + \alpha_h\beta_k + \alpha_{h-1}\beta_{k+1} + \cdots,$$

da sie bis auf das durch p nicht teilbare Glied $\alpha_h\beta_k$ aus lauter nach der Annahme durch p teilbaren Summanden besteht, durch p nicht teilbar sein; da die linke Seite der Gleichung (22) aber durch p aufgeht, muß notwendig γ_0 durch p teilbar sein und daher der Primfaktor p aus $\alpha_0\beta_0$ gegen γ_0 sich heben. So hebt sich denn das ganze Produkt $\alpha_0\beta_0$ gegen γ_0 auf, während dabei auch in γ_0 kein Faktor verbleiben kann, da sonst alle Koeffizienten von $C'(x)$ diesen gemeinsam hätten. Also ergibt sich die Gleichheit

$$\alpha_0\beta_0 = \gamma_0, \tag{24}$$

derzufolge unter den Voraussetzungen des Gaussischen Satzes der Generalnenner γ_0 der Koeffizienten von $C(x)$ nicht gleich 1, d. h., wie der Satz es behauptet, diese Koeffizienten nicht sämtlich ganze rationale Zahlen sein können.

Aus diesem Gaussischen Satze erhellt die Richtigkeit der früher (Kap. 3, Nr. 4) benutzten Bemerkung, daß eine ganze Funktion von x mit ganzzahligen Koeffizienten, deren höchster gleich 1, wenn sie nicht in Faktoren mit ebenfalls ganzzahligen Koeffizienten zerlegbar ist, es auch nicht ist in Faktoren, deren Koeffizienten rationale Zahlen sind.

Wegen (24) aber nimmt die Gleichung (22) die Gestalt

$$C'(x) = A'(x)\,B'(x)$$

an und lehrt den ferneren Satz, daß das Produkt zweier ursprünglichen Funktionen wieder eine ursprüngliche Funktion ist.

Ist nun

$$A(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$$

eine ganze Funktion mit beliebigen rationalen Koeffizienten, deren erster a_0 positiv gedacht werde, so gibt es eine ganz bestimmte positive rationale Zahl t von der Beschaffenheit, daß $\frac{A(x)}{t}$ eine ursprüngliche Funktion wird; in der Tat, wenn $a_i = \frac{\alpha_i}{\alpha}$ gesetzt, und unter α der Generalnenner aller a_i, unter δ aber der größte gemeinsame Teiler aller α_i verstanden wird, so wird $t = \frac{\delta}{\alpha}$ die gedachte Zahl sein. Nennt man diese so bestimmte Zahl t den **Teiler der Funktion** $A(x)$, so besteht folgender Satz:

Der Teiler eines Produkts zweier ganzen Funktionen von x ist das Produkt aus den Teilern der Faktoren. Setzt man nämlich

$$A(x) = t \cdot A'(x),\ B(x) = \tau \cdot B'(x), \tag{25}$$

wo t, τ die Teiler der ganzen Funktionen $A(x)$, $B(x)$, also $A'(x)$, $B'(x)$ ursprüngliche Funktionen bedeuten, so wird das Produkt

$$C(x) = A(x) \cdot B(x)$$

sich schreiben lassen, wie folgt:

$$\theta \cdot C'(x) = t\tau \cdot A'(x)\, B'(x),$$

wo θ den Teiler von $C(x)$, also $C'(x)$ eine ursprüngliche Funktion bedeutet. Da dem vorauf Bewiesenen zufolge auch $A'(x)\, B'(x)$ eine ursprüngliche Funktion ist, liefert diese Gleichung notwendig die andere:

$$\theta = t\tau \tag{26}$$

und damit den Beweis der Behauptung.

Sind daher alle Koeffizienten der Funktionen

$$\begin{aligned} A(x) &= a_0 x^m + a_1 x^{m-1} + \cdots + a_m \\ B(x) &= b_0 x^n + b_1 x^{n-1} + \cdots + b_n \end{aligned} \tag{27}$$

rationale Zahlen und alle Koeffizienten ihres Produktes

$$C(x) = c_0 x^{m+n} + c_1 x^{m+n-1} + \cdots + c_{m+n} \tag{28}$$

ganze Zahlen, so sind auch sämtliche Produkte $a_i b_k$ ganze Zahlen. In der Tat, wenn wieder die Gleichungen (25), sowie die Gleichung

$$C(x) = \theta \cdot C'(x)$$

angesetzt werden, wo $A'(x)$, $B'(x)$, $C'(x)$ ursprüngliche Funktionen bedeuten, so hat jedes der Produkte $a_i b_k$ die Gestalt $t a_i' \cdot \tau b_k'$, ist also wegen (26) gleich $\theta \cdot a_i' b_k'$, wo sowohl θ als Teiler einer ganzzahligen Funktion als auch $a_i' b_k'$ ganzzahlig sind, und ist demnach ebenfalls eine ganze Zahl.

Es wäre nun eine einfache und naheliegende Verallgemeinerung dieses letzten Satzes, welcher im Grunde dem Gaussischen gleichbedeutend ist, wenn wir ihn aussprächen, wie folgt:

Wenn das Produkt zweier ganzen Funktionen (27) mit algebraischen Koeffizienten lauter *ganze* algebraische Koeffizienten hat, so ist auch jedes aus einem Koeffizienten von $A(x)$ und einem Koeffizienten von $B(x)$ gebildete Produkt eine *ganze* algebraische Zahl.

Gesetzt, dieser Satz bestände, so würde man weiter aus ihm folgern, daß, wenn die Koeffizienten des Produkts Vielfache einer ganzen Zahl γ sind, auch die sämtlichen Produkte $a_i b_k$ solche Vielfache sein müssen. Denn, setzt man allgemein $c_i = \gamma \gamma_i$ und $a_i = \gamma \alpha_i$, so wird die Funktion

$$\gamma_0 x^{m+n} + \gamma_1 x^{m+n-1} + \cdots + \gamma_{m+n}$$

das Produkt der beiden Funktionen

$$\alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$$
$$b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

sein, deren Koeffizienten algebraische Zahlen sind; werden also die γ_i sämtlich als ganze algebraische Zahlen gedacht, so müssen es dem vorausgesetzten Satze zufolge auch alle Produkte $\alpha_i b_k$, d. h. alle Produkte $a_i b_k$ müssen Vielfache von γ sein.

Dieser letztere Satz nun ist von *A. Hurwitz*[1])

1) A. Hurwitz, Über die Theorie der Ideale, Götting. Nachr. 1894, Nr. 4.

als die Quelle nachgewiesen worden, aus der man sogleich den fundamentalen Satz der Theorie der algebraischen Zahlen, um den es sich handelt, entnehmen kann. In der Tat, sei das gegebene Ideal $\mathfrak{j}$ des Körpers n^{ten} Grades als n-gliedriger Modulus in $\mathfrak{g}$ dargestellt durch

$$(29)\qquad \mathfrak{j} = [\alpha_1, \alpha_2, \cdots, \alpha_n],$$

wo also die α_i sämtlich ganze Zahlen des Körpers sind, und man setze

$$A(x) = \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_n.$$

Indem unter $\alpha_i^{(1)}, \alpha_i^{(2)}, \cdots, \alpha_i^{(n-1)}$ die zu α_i konjugierten Zahlen verstanden werden, bilde man die zu $A(x)$ konjugierten Funktionen $A^{(1)}(x)$, $A^{(2)}(x)$, $\cdots$, $A^{(n-1)}(x)$ und deren Produkt, welches kurz

$$B(x) = \beta_1 x^{r-1} + \beta_2 x^{r-2} + \cdots + \beta_r$$

genannt werde; endlich setze man

$$C(x) = A(x)\, B(x) = \gamma_1 x^{s-1} + \gamma_2 x^{s-2} + \cdots + \gamma_s.$$

Ist nun $f_i(x) = 0$ die ganzzahlige Gleichung, der α_i genügt, so sind die zu α_i konjugierten Zahlen $\alpha_i^{(1)}, \alpha_i^{(2)}, \cdots, \alpha_i^{(n-1)}$ die Wurzeln der Gleichung $\frac{f_i(x)}{x - \alpha_i} = 0$, deren Koeffizienten ganze, ganzzahlige Funktionen von α_i sind; die Koeffizienten β_i werden daher (wie aus der Anmerkung zum Schlusse des 1. Kapitels sich unschwer ergibt) als symmetrische ganze, ganzzahlige Funktionen von den Wurzeln jeder dieser abgeleiteten Gleichungen ganze, ganzzahlige Funktionen der Zahlen α_i, also ganze Zahlen des Körpers sein. Desgleichen ergeben sich die Koeffizienten γ_i als symmetrische ganze, ganzzahlige Funktionen von allen Wurzeln jeder der Gleichungen $f_i(x) = 0$ gleich rationalen ganzen Zahlen. Nun kann man in dem in Kap. 4 dem Symbole beigelegten Sinne auch setzen

$$(30)\qquad \mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\},$$

denn jede Zahl des Ideals (29) ist auch eine Zahl von der Form

$$(31)\qquad \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n,$$

wo die γ_i Zahlen in $\mathfrak{g}$ bedeuten, aber auch umgekehrt ist nach

der Definition eines Ideals jedes Produkt $\gamma_i \alpha_i$, also auch jede Zahl von der Form (31) im Ideale (29) enthalten. Versteht man dann ferner unter $\mathfrak{j}'$ das Ideal

$$\mathfrak{j}' = \{\beta_1, \beta_2, \cdots, \beta_r\},$$

so wird

$$\mathfrak{j}\mathfrak{j}' = \{\cdots, \alpha_i \beta_k, \cdots\} \tag{32}$$

sein. Nennt man aber γ den größten gemeinsamen Teiler der Koeffizienten γ_i, der eine rationale, also auch algebraische ganze Zahl ist, so müssen nach dem Hilfssatze von Hurwitz sämtliche Elemente $\alpha_i \beta_k$ des Ideals (32) Vielfache von γ und somit $\mathfrak{j}\mathfrak{j}'$ im Hauptideale $\mathfrak{g}\gamma$ enthalten sein. Da aber

$$\gamma = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_s u_s$$

gesetzt werden kann, wo die u_i rationale ganze Zahlen bezeichnen, so folgt wegen

$$\gamma_1 = \alpha_1 \beta_1, \ \gamma_2 = \alpha_1 \beta_2 + \alpha_2 \beta_1, \ \gamma_3 = \alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1, \cdots$$

die Beziehung

$$\gamma = u_1 \cdot \alpha_1 \beta_1 + u_2(\alpha_1 \beta_2 + \alpha_2 \beta_1) + u_3(\alpha_1 \beta_3 + \alpha_2 \beta_2 + \alpha_3 \beta_1) + \cdots,$$

welche lehrt, daß umgekehrt γ und somit auch das ganze Ideal $\mathfrak{g}\gamma$ im Ideale $\mathfrak{j}\mathfrak{j}'$ enthalten sein muß. Mithin ergibt sich

$$\mathfrak{j} \cdot \mathfrak{j}' = \mathfrak{g}\gamma,$$

eine Gleichung, wie sie nachgewiesen werden sollte.

Hurwitz hat seinen Hilfssatz mittels der Theorie der symmetrischen Funktionen bewiesen. Wir ziehen hier vor, ihn als Korollar des voraufgestellten, bisher hypothetischen Satzes aufzufassen, und gehen daher dazu über, zu zeigen, wie dieser bewiesen werden kann.

4. Wir folgen dabei zuerst den Spuren Dedekinds.[1])

Sei

$$f(x) = c_0 x^s + c_1 x^{s-1} + \cdots + c_s \tag{33}$$

1) R. Dedekind, Über einen arithmetischen Satz von Gauss, Mittheil. der deutschen mathem. Ges. in Prag 1892.

eine ganze Funktion von x mit algebraisch ganzzahligen Koeffizienten c_i und ω irgend eine Wurzel der Gleichung

$$f(x) = 0. \tag{34}$$

Setzt man dann für $i = 0, 1, 2, \cdots, s$

$$C_i = c_0\omega^i + c_1\omega^{i-1} + \cdots + c_i, \tag{35}$$

so ergibt sich zuerst die Rekursionsformel

$$C_{i+1} - C_i \cdot \omega = c_{i+1}, \tag{36}$$

mittels deren die Zahlen $C_0, C_1, C_2, \cdots$ der Reihe nach aus den Koeffizienten c_i und dem Anfangsgliede

$$C_0 = c_0$$

gebildet werden können. Ferner erhält man mit Rücksicht darauf, daß

$$c_0\omega^s + c_1\omega^{s-1} + \cdots + c_s = 0 \tag{37}$$

ist, folgende Reihe von Gleichungen:

$$\left\{\begin{aligned}
C_i &= c_0\omega^i + c_1\omega^{i-1} + \cdots + c_i\\
C_i\,\omega &= c_0\omega^{i+1} + c_1\omega^i + \cdots + c_i\omega\\
&\cdots\cdots\cdots\cdots\\
C_i\omega^{s-i-1} &= c_0\omega^{s-1} + c_1\omega^{s-2} + \cdots + c_i\omega^{s-i-1}\\
C_i\omega^{s-i} &= -c_{i+1}\omega^{s-i-1} - c_{i+2}\omega^{s-i-2} - \cdots - c_s\\
C_i\omega^{s-i+1} &= -c_{i+1}\omega^{s-i} - c_{i+2}\omega^{s-i-1} - \cdots - c_s\omega\\
&\cdots\cdots\cdots\cdots\\
C_i\omega^{s-1} &= -c_{i+1}\omega^{s-2} - c_{i+2}\omega^{s-3} - \cdots - c_s\omega^{i-1}\\
C_i\omega^s &= -c_{i+1}\omega^{s-1} - c_{i+2}\omega^{s-2} - \cdots - c_s\omega^i.
\end{aligned}\right. \tag{38}$$

Alle diese Gleichungen sind linear in Bezug auf die Potenzen $1, \omega, \omega^2, \cdots, \omega^{s-1}$ und haben algebraisch ganzzahlige Koeffizienten. Eliminiert man daher jene Potenzen aus den ersten s der Gleichungen, so erkennt man nach schon bekannter Schlußweise, daß die Zahl C_i, und ebenso durch Elimination jener Potenzen aus den letzten s Gleichungen, daß die Zahl $C_i\omega$ einer Gleichung Genüge leistet, deren Koeffizienten algebraische ganze Zahlen sind, der höchste derselben gleich Eins, daß somit jede von ihnen eine ganze algebraische Zahl sein muß.

Diesem Resultate geben wir zunächst einen zwiefachen Ausdruck:

Zuerst dürfen wir den Satz aussprechen: Hat die Gleichung

$$f(x) = 0$$

ganze algebraische Koeffizienten und die Wurzel ω, so sind auch die Koeffizienten der Funktion

$$\frac{f(x)}{x - \omega}$$

ganze algebraische Zahlen. In der Tat, setzt man

$$\frac{f(x)}{x - \omega} = C_0 x^{s-1} + C_1 x^{s-2} + \cdots + C_{s-1},$$

so sind die Koeffizienten C_i genau durch die Formel (35) bestimmt.

Sei ferner

$$\mathfrak{m} = [\alpha, \beta] \tag{39}$$

ein zweigliedriger Modulus, dessen Elemente α, β irgend welche algebraische Zahlen sind, so leistet der Quotient $\omega = \frac{\alpha}{\beta}$, da er gleichfalls eine algebraische Zahl ist, einer Gleichung von der Form (34) Genüge, deren Koeffizienten c_i ganze rationale Zahlen sind, die ohne gemeinsamen Teiler vorausgesetzt werden können oder 1 zum größten gemeinsamen Teiler haben. Nach Kap. 3, Nr. 1 ist demnach der Modulus

$$[c_0, c_1, c_2, \cdots, c_s]$$

gleich dem Modulus [1], den wir $\mathfrak{z}$ genannt haben, in Zeichen:

$$[c_0, c_1, c_2, \cdots, c_s] = \mathfrak{z}. \tag{40}$$

Setzt man nun $C_i = \beta \nu_i$, so wird $C_i \omega = \alpha \nu_i$ und dem vorher erhaltenen Resultate zufolge sind diese Zahlen $\alpha \nu_i$, $\beta \nu_i$ ganze algebraische Zahlen, zwischen denen übrigens (s. (36)) die Beziehungen

$$\beta \nu_0 = c_0, \; \beta \nu_{i+1} - \alpha \nu_i = c_{i+1} \tag{41}$$

stattfinden, denen gemäß die Zahlen $\nu_0, \nu_1, \nu_2, \cdots, \nu_s$ rational durch die Zahlen α, β ausdrückbar sind. Zudem wird wegen

eben dieser Beziehungen der Modulus $\mathfrak{z}$ im Modulus $\mathfrak{m} \cdot \mathfrak{n}$ enthalten sein, wenn

$$(42) \qquad \mathfrak{n} = [\nu_0, \nu_1, \nu_2, \cdots, \nu_s]$$

gesetzt wird, woraus hervorgeht, daß $\mathfrak{n}$ nicht aus lauter der Null gleichen Zahlen bestehen kann, während der Modulus

$$(43) \qquad \mathfrak{m} \cdot \mathfrak{n} = [\cdots, \alpha\nu_i, \cdots, \beta\nu_i, \cdots]$$

nur ganze algebraische Zahlen enthält. Somit erlangen wir folgende zweite Deutung des vorher gefundenen Resultates:

Jeder zweigliedrige Modulus $\mathfrak{m}$, dessen Elemente algebraische Zahlen sind, kann durch Multiplikation mit einem von Null verschiedenen Modulus $\mathfrak{n}$, dessen Zahlen rational aus denen von $\mathfrak{m}$ gebildet sind, in einen Modulus $\mathfrak{m} \cdot \mathfrak{n}$ verwandelt werden, der nur ganze algebraische Zahlen, unter ihnen die sämtlichen Zahlen des Modulus $\mathfrak{z}$, enthält.

Die erste Fassung bietet nun die Handhabe, den in Frage stehenden Satz der vorigen Nummer in einfacher Weise zu begründen. Man schreibe die Funktion (28), in ihre Linearfaktoren zerlegt,

$$(44) \qquad C(x) = c_0(x - \omega_1)(x - \omega_2) \cdots (x - \omega_{m+n})$$

sodaß $\omega_1, \omega_2, \cdots, \omega_{m+n}$ ihre Wurzeln bezeichnen. Durch wiederholte Anwendung des erst ausgesprochenen Satzes findet sich dann: Hat die Funktion (44) algebraisch ganze Koeffizienten, so behält sie solche auch nach Division mit einer beliebigen Anzahl ihrer Linearfaktoren. Die letzten Koeffizienten der so entstehenden Funktionen sind aber die sämtlichen Produkte von der Form

$$c_0 \cdot \omega_h \omega_i \omega_k \cdots,$$

wo $\omega_h, \omega_i, \omega_k, \cdots$ beliebige und beliebig viele der Wurzeln bedeuten, und sind also die sämtlichen Glieder $c_0\omega'$ des entwickelten Produktes

$$c_0(1 + \omega_1)(1 + \omega_2) \cdots (1 + \omega_{m+n})$$

und nach dem gedachten Satze ganze algebraische Zahlen. Setzt man aber ebenso die Funktionen (27), als deren Produkt $C(x)$ gedacht wird, in die Formen

$$A(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)$$
$$B(x) = b_0(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n),$$

so sind die α_i und die β_i zusammen genommen die Wurzeln ω_i, und, wenn man $a_0\alpha'$, $b_0\beta'$ die allgemeinen Glieder der entwickelten Produkte

$$a_0(1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_m)$$
$$b_0(1 + \beta_1)(1 + \beta_2) \cdots (1 + \beta_n)$$

nennt, so werden wegen $a_0 b_0 = c_0$ die sämtlichen Glieder $c_0\omega'$ mit den sämtlichen Produkten $a_0\alpha' \cdot b_0\beta'$ identisch, die letztern demnach ganze algebraische Zahlen sein. Nun ist aber jeder Koeffizient a_i der Funktion $A(x)$ ein Aggregat von Gliedern von der Form $a_0\alpha'$, jeder Koeffizient b_k der Funktion $B(x)$ ein solches von Gliedern von der Form $b_0\beta'$, und somit jedes Produkt $a_i b_k$ ein Aggregat von Gliedern von der Form $a_0\alpha' \cdot b_0\beta'$, demnach auch, wie der Satz der vorigen Nummer behauptet, eine ganze algebraische Zahl.

5. Dieser einfache Dedekindsche Beweis benutzt die Zerlegbarkeit der ganzen Funktion einer Veränderlichen in Linearfaktoren. Obwohl wir darin keinen Mangel erblicken können, da diese Zerlegbarkeit nur eine einfache algebraische Folgerung der, der ganzen Theorie der algebraischen Zahlen zum Grunde liegenden Tatsache ist, daß jede solche ganze Funktion eine Wurzel besitzt, wollen wir doch noch einen zweiten *Dedekind*schen Beweis desselben Satzes, der dieser Eigenschaft ganzer Funktionen nicht bedarf, hier mitteilen, da er nicht nur tiefer zurückgeht in die Elemente der Modultheorie, sondern auch zu weiteren Betrachtungen Anlaß gibt.[1])

Sei

$$\mathfrak{a} = [a_0, a_1, a_2, \cdots, a_m],$$

so wird $\mathfrak{a}^{n+1}$ ebenfalls ein endlicher Modulus sein, dessen Elemente die sämtlichen Produkte aus $n + 1$ gleichen oder verschiedenen Faktoren aus der Reihe $a_0, a_1, a_2, \cdots, a_m$ sind. Jedes derselben hat also den Ausdruck

---

1) Dedekind, an der zuletzt zitierten Stelle.

(45) $$a_{i_0} \cdot a_{i_1} \cdot a_{i_2} \cdots a_{i_n},$$

wo $i_0, i_1, i_2, \cdots, i_n$ gleiche oder verschiedene Zahlen der Reihe $0, 1, 2, \cdots, m$ sind, die man sich der Größe nach geordnet denken kann, sodaß

$$i_0 \overline{\overline{<}} i_1 \overline{\overline{<}} i_2 \overline{\overline{<}} \cdots \overline{\overline{<}} i_n$$

sei. Setzt man $r_k = i_k + k$, so werden die Zahlen $r_0, r_1, r_2, \cdots, r_n$ eine Kombination von $n+1$ nach der Größe geordneten Zahlen der Reihe $0, 1, 2, \cdots, m+n$ bilden, welche kurz die Kombination r heiße, und das dieser Kombination entsprechende Produkt (45) soll kurz

(46) $$\alpha_r = a_{r_0} \cdot a_{r_1 - 1} \cdot a_{r_2 - 2} \cdots a_{r_n - n}$$

genannt werden. Man erhält aber aus dieser Formel auch umgekehrt eins der Elemente (45) des Modulus $\mathfrak{a}^{n+1}$, welche der gedachten Kombinationen man r auch bedeuten läßt. Denn, ist

$$r_0 < r_1 < r_2 < \cdots < r_n$$

eine derartige Kombination, so ist, wenn wieder $r_k = i_k + k$ gesetzt wird, zugleich auch

$$i_0 \overline{\overline{<}} i_1 \overline{\overline{<}} i_2 \overline{\overline{<}} \cdots \overline{\overline{<}} i_n$$

eine der Größe nach geordnete Kombination von gleichen oder ungleichen Zahlen der Reihe $0, 1, 2, \cdots, m$, und α_r wird zum Ausdrucke (45). Wir werden nun von zwei Gliedern $\alpha_r, \alpha_{r'}$ von der Form (46) das zweite das niedrigere nennen, wenn der erste der Indizes $r_0', r_1', r_2', \cdots, r_n'$, welcher von dem entsprechenden Index $r_0, r_1, r_2, \cdots, r_n$ verschieden ist, kleiner ist als der letztere; von allen Elementen des Modulus $\mathfrak{a}^{n+1}$ wäre so offenbar a_0^{n+1} das niedrigste, a_m^{n+1} das höchste Glied.

Dies vorausgeschickt, kommen wir überein, unter dem Zeichen a_i die Null zu verstehen, sooft der positiv oder negativ gedachte Index i der Reihe $0, 1, 2, \cdots, m$ nicht angehört und ordnen jedem Produkte α_r eine Determinante zu, deren Hauptglied α_r ist, durch die Formel

(47) $$\alpha_r' = \begin{vmatrix} a_{r_0}, & a_{r_0 - 1}, & \cdots, & a_{r_0 - n} \\ a_{r_1}, & a_{r_1 - 1}, & \cdots, & a_{r_1 - n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{r_n}, & a_{r_n - 1}, & \cdots, & a_{r_n - n} \end{vmatrix};$$

offenbar ist sie ein Aggregat gewisser Produkte von der Form (46), unter denen das Hauptglied das höchste ist. Nun besteht für jeden endlichen Modulus die Gleichheit

$$[\alpha_0, \alpha_1, \alpha_2, \cdots] = [\alpha + \alpha_0, \alpha_1, \alpha_2, \cdots],$$

so oft α ein Aggregat der übrigen Elemente $\alpha_1, \alpha_2, \cdots$ ist, denn, da offenbar die Elemente eines jeden dieser beiden Moduln auch Zahlen des andern sind, so sind überhaupt alle in dem einen von ihnen enthaltenen Zahlen auch im andern enthalten, und umgekehrt. Indem man diese Bemerkung auf den Modulus

$$\mathfrak{a}^{n+1} = [\cdots, \alpha_{r'}, \cdots, \alpha_r, \cdots]$$

zur Anwendung bringt, dessen Elemente die sämtlichen Produkte (46) sind, darf man zunächst das höchste dieser Elemente, welches ein Aggregat aus der ihm entsprechenden Determinante und niedrigeren Gliedern ist, einfach durch diese Determinante ersetzen, und indem man dann mit dem nächstniedrigen Gliede gleicherweise verfährt usw., findet man schließlich die Gleichung

$$\mathfrak{a}^{n+1} = [\cdots, \alpha'_{r'}, \cdots, \alpha'_r, \cdots],$$

durch welche die ursprüngliche Gestalt des Modulus $\mathfrak{a}^{n+1}$ in zweckentsprechender Weise verwandelt ist.

Es soll nämlich jetzt bewiesen werden, daß, wenn

$$\mathfrak{a} = [a_0, a_1, a_2, \cdots, a_m]$$
$$\mathfrak{b} = [b_0, b_1, b_2, \cdots, b_n]$$
$$\mathfrak{c} = [c_0, c_1, c_2, \cdots, c_{m+n}]$$

die aus den Koeffizienten der drei ganzen Funktionen

$$A(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m$$
$$B(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n$$
$$C(x) = A(x) \cdot B(x) = c_0x^{m+n} + c_1x^{m+n-1} + \cdots + c_{m+n}$$

gebildeten Moduln bedeuten, jede der beiden Gleichungen

$$\mathfrak{a}^{n+1} \cdot \mathfrak{b} = \mathfrak{a}^n \cdot \mathfrak{c}, \quad \mathfrak{a} \cdot \mathfrak{b}^{m+1} = \mathfrak{b}^m \cdot \mathfrak{c}$$

stattfindet. Es genügt, die eine derselben zu beweisen. Zu diesem Zwecke bemerke man zuerst, daß nach der Bildungsweise des Produktes $C(x)$ und mit Rücksicht auf die bezüglich der a_i getroffenen Übereinkunft

$$(48) \qquad c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_{i-n} b_n$$

gesetzt werden darf. Dieser Gleichung zufolge ist

$$(49) \qquad \mathfrak{c} \succ \mathfrak{a}\mathfrak{b}, \quad \text{also auch} \quad \mathfrak{a}^n \cdot \mathfrak{c} \succ \mathfrak{a}^{n+1} \cdot \mathfrak{b}.$$

Bildet man ferner aus der Formel (47) das Produkt $\alpha_r' \cdot b_k$, indem man die Kolonne mit den Elementen

$$a_{r_0 - k}, a_{r_1 - k}, \cdots, a_{r_n - k}$$

mit b_k multipliziert, so darf nach einfachen Determinantensätzen diese Kolonne mit Rücksicht auf (48) durch $c_{r_0}, c_{r_1}, \cdots, c_{r_n}$ ersetzt werden und dann ergibt sich

$$\alpha_r' \cdot b_k = \alpha'_{r,0} \cdot c_{r_0} + \alpha'_{r,1} \cdot c_{r_1} + \cdots + \alpha'_{r,n} \cdot c_{r_n},$$

während die $\alpha'_{r,i}$ gewisse Unterdeterminanten n^{ten} Grades der Determinante (47) bedeuten, welche als Aggregate von Produkten von je n der Größen a_i offenbar Zahlen des Modulus $\mathfrak{a}^n$ sind. Hieraus ist zu schließen, daß die sämtlichen Produkte $\alpha_r' \cdot b_k$, welche die Elemente des Modulus $\mathfrak{a}^{n+1} \cdot \mathfrak{b}$ bilden, und somit auch dieser ganze Modulus im Modulus $\mathfrak{a}^n \cdot \mathfrak{c}$ enthalten sind:

$$\mathfrak{a}^{n+1} \cdot \mathfrak{b} \succ \mathfrak{a}^n \cdot \mathfrak{c}.$$

In Verbindung mit (49) findet sich demnach die behauptete Gleichheit

$$\mathfrak{a}^{n+1} \cdot \mathfrak{b} = \mathfrak{a}^n \cdot \mathfrak{c}.$$

Bis hierher galten unsere Betrachtungen für jede Beschaffenheit der Koeffizienten a_i, b_i, c_i. Wir setzen nun voraus, die Koeffizienten c_i seien ganze algebraische Zahlen; dann werden auch alle Zahlen des Modulus $\mathfrak{c}$ solche Zahlen sein. Nun bezeichne man mit

$$\alpha^{(0)}, \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(\nu)}$$

eine Basis des Moduls $\mathfrak{a}^n$; da alle Zahlen

$$a_i b_k \cdot \alpha^{(0)}, \; a_i b_k \cdot \alpha^{(1)}, \cdots, a_i b_k \cdot \alpha^{(\nu)}$$

dem Modulus $\mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{a}^n = \mathfrak{a}^{n+1} \cdot \mathfrak{b} = \mathfrak{a}^n \cdot \mathfrak{c}$ angehören, so ist jede jener Zahlen eine lineare Funktion der Basiszahlen

$$\alpha^{(0)}, \alpha^{(1)}, \cdots, \alpha^{(\nu)}$$

mit Koeffizienten, welche dem Modulus $\mathfrak{c}$ angehören, also ganze algebraische Zahlen sind. Daraus schließt man aber in schon gewohnter Weise, daß auch $a_i b_k$ eine ganze algebraische Zahl

ein muß, also aufs neue die Richtigkeit des zu Beweis stehenden Satzes.

6. Ohne aber über die Beschaffenheit der Koeffizienten c_i irgend welche besonderen Voraussetzungen zu machen, entnimmt man der letzten Betrachtung das allgemeine Resultat:

Das Produkt $a_i b_k$ aus irgend einem Koeffizienten der ganzen Funktion $A(x)$ in irgend einen Koeffizienten der ganzen Funktion $B(x)$ ist Wurzel einer Gleichung, deren höchster Koeffizient gleich 1, die übrigen ganze, ganzzahlige Funktionen der Koeffizienten des Produkts $C(x) = A(x) \cdot B(x)$ sind. In dieser Verallgemeinerung findet er sich bei Hurwitz (über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen, Götting. Nachr. 1895, Heft 2), doch auch früher schon, wenngleich in anderer Einkleidung, bei Kronecker (Berliner Sitzgsber. 1883, p. 957), sowie auch bei Molk (Acta Math. 6, p. 71).[1] An derselben Stelle gibt Hurwitz auch einen, von dem vorigen verschiedenen, bemerkenswerten Beweis des Satzes. Des leichteren Ausdrucks wegen wollen wir dabei nach seinem Vorgange uns einer Bezeichnung bedienen, welche Mertens (Wiener Sitzgsber. 1894, p. 6) vorgeschlagen hat. Dieser nennt jede in einem endlichen Modul $[\alpha_1, \alpha_2, \cdots, \alpha_m]$ enthaltene Größe, nämlich jede ganzzahlige homogene lineare Funktion von $\alpha_1, \alpha_2, \cdots, \alpha_m$ eine „Vielfachsumme" dieser Elemente. Bedeutet daher dann $a^{(r)}$ jedes Produkt aus r gleichen oder verschiedenen der Koeffizienten a_i, so kann man dem allgemeinen Modulsatze der vorigen Nummer die Deutung geben, daß jeder Ausdruck $a^{(n+1)} \cdot b^{(1)}$ eine Vielfachsumme der Produkte $a^{(n)} \cdot c^{(1)}$ sei; eine neue Begründung dieses Ausspruchs liefert daher auch einen neuen Beweis des zuvor ausgesprochenen Satzes.

Nun erkennt man zunächst leicht die Giltigkeit des folgenden Hilfssatzes:

Sind G, H ganze rationale Funktionen von be-

---

1) Man beachte die Begründung dieses Kroneckerschen Fundamentalsatzes und des Satzes von Dedekind bei J. König, Einleitung in die allgemeine Theorie der algebraischen Größen, 1903, p. 74 ff.

liebig vielen Veränderlichen $t_0, t_1, t_2, \cdots$ von der Beschaffenheit, daß

$$(50) \qquad \Delta \cdot H = G,$$

und Δ ein Produkt aus irgend welchen der Differenzen

$$t_0 - t_1,\ t_0 - t_2,\ \cdots,\ t_1 - t_2,\ \cdots$$

ist, so sind die Koeffizienten von H Vielfachsummen der Koeffizienten von G.

Dies folgt sofort durch wiederholte Anwendung des der besonderen Annahme $\Delta = t_0 - t_1$ entsprechenden Satzes. Bei dieser Annahme aber nimmt die vorausgesetzte Gleichung (50) die Gestalt an

$$(t_0 - t_1) \cdot H = G$$

und liefert, wenn, nach Potenzen von t_0 geordnet,

$$G = G_0 + t_0 G_1 + t_0^2 G_2 + \cdots$$

gesetzt wird, die andere Gleichung

$$(t_0 - t_1) H = (t_0 - t_1) G_1 + (t_0^2 - t_1^2) G_2 + \cdots$$

oder

$$H = G_1 + (t_0 - t_1) G_2 + (t_0^2 + t_0 t_1 + t_1^2) G_3 + \cdots,$$

woraus, wenn man rechts wieder diejenigen Glieder zusammengefaßt denkt, welche gleiche Produkte der t_i enthalten, jeder Koeffizient von H wirklich als eine Vielfachsumme von Koeffizienten von G hervorgeht.

Dies vorausgeschickt, schließt man, wenn die drei ganzen Funktionen $A(x)$, $B(x)$, $C(x)$ durch die Gleichung

$$C(x) = A(x) \cdot B(x)$$

miteinander verbunden sind, mithin $B(x) = \frac{C(x)}{A(x)}$ ist, aus der Interpolationsformel von Lagrange, nach welcher

$$B(x) = \frac{C(t_0)}{A(t_0)} \cdot \frac{(x - t_1) \cdots (x - t_n)}{(t_0 - t_1) \cdots (t_0 - t_n)} + \cdots + \frac{C(t_n)}{A(t_n)} \cdot \frac{(x - t_0) \cdots (x - t_{n-1})}{(t_n - t_0) \cdots (t_n - t_{n-1})}$$

gesetzt werden darf, durch Multiplikation mit den Nennern nachstehende Beziehung:

$$\Delta \cdot A(t_0) \cdots A(t_n) \cdot B(x) = G(x;\ t_0, t_1, \cdots, t_n);$$

in ihr bedeutet Δ das für die Veränderlichen $t_0, t_1, \cdots, t_n$ gebildete Differenzenprodukt, und die Koeffizienten der ganzen Funktion G sind offenbar Vielfachsummen der Produkte $a^{(n)} \cdot c^{(1)}$.

Nach dem Hilfssatze müssen daher auch die Koeffizienten des Produktes

$$A(t_0)\cdots A(t_n)\cdot B(x)$$

solche Vielfachsummen von $a^{(n)}\cdot c^{(1)}$ sein, und da sich unter ihnen alle Produkte von der Form $a^{(n+1)}\cdot b^{(1)}$ befinden, so ist damit der verheißene neue Beweis unseres Satzes erlangt.

Der Satz ist aber nicht auf Funktionen von nur einer Veränderlichen beschränkt, sondern gilt für ganze Funktionen von beliebig viel Veränderlichen. In der Tat, sind

$$A(x_i)=\sum a_{\alpha_1,\alpha_2,\cdots,\alpha_m}\cdot x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m}$$
$$B(x_i)=\sum b_{\beta_1,\beta_2,\cdots,\beta_m}\cdot x_1^{\beta_1}x_2^{\beta_2}\cdots x_m^{\beta_m}$$

zwei ganze Funktionen der Veränderlichen $x_1, x_2, \cdots, x_m$ und $C(x_i)$ ihr Produkt, so kann man, indem man mit g eine positive ganze Zahl bezeichnet, welche größer gedacht werde, als alle in den drei Funktionen auftretenden Exponenten, durch die Substitution

$$x_1=x,\ x_2=x^g,\ x_3=x^{g^2},\ \cdots,\ x_m=x^{g^{m-1}}$$

die Funktionen $A(x_i)$, $B(x_i)$, $C(x_i)$, wie sich ohne Mühe überblicken läßt, in drei ganze Funktionen $\bar{A}(x)$, $\bar{B}(x)$, $\bar{C}(x)$ der einen Veränderlichen x überführen, deren einzelne Potenzen eben dieselben Koeffizienten haben, wie die entsprechenden Glieder jener Funktionen, während aus der vorausgesetzten Gleichung

$$C(x_i)=A(x_i)B(x_i)$$

sich

$$\bar{C}(x)=\bar{A}(x)\bar{B}(x)$$

ergibt. Bezeichnen nun wieder a_i, b_i, c_i die Koeffizienten von $\bar{A}(x)$, $\bar{B}(x)$, $\bar{C}(x)$, d. h. von $A(x_i)$, $B(x_i)$, $C(x_i)$ resp., und n den Grad der Funktion $\bar{B}(x)$, so sind dem vorigen Satze zufolge alle Produkte $a^{(n+1)}\cdot b^{(1)}$ Vielfachsummen der Produkte $a^{(n)}\cdot c^{(1)}$, man darf also den allgemeineren Satz aussagen:

Bedeuten $A(x_i)$, $B(x_i)$ ganze Funktionen von beliebig viel Veränderlichen x_i und mit den Koeffizienten a_i, b_i resp., und $C(x_i)$ ihr Produkt mit den Koeffizienten c_i, so gibt es eine positive ganze Zahl n

von der Beschaffenheit, daß die Produkte $a^{(n+1)} \cdot b^{(1)}$ Vielfachsummen der Produkte $a^{(n)} \cdot c^{(1)}$ sind. Da im übrigen jeder Koeffizient c_i eine Vielfachsumme der Produkte $a_i b_k$, also alle Produkte $a^{(n)} \cdot c^{(1)}$ stets umgekehrt auch Vielfachsummen der Produkte $a^{(n+1)} \cdot b^{(1)}$ sind, kommt dieser Satz auf die Gleichheit der beiden Moduln $\mathfrak{a}^{n+1} \cdot \mathfrak{b}$, $\mathfrak{a}^n \cdot \mathfrak{c}$, in denen $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ die endlichen Moduln mit den Elementen a_i, b_i, c_i resp. bedeuten, für einen hinreichend großen Exponenten n zurück.

Es leuchtet ein, daß, wenn jene Gleichheit für einen Exponenten n besteht, sie auch für jeden noch größeren Exponenten stattfinden muß. Aus dem Beweise des Satzes ging n als der Grad hervor, zu welchem die Funktion $B(x_i)$ durch die angewandte Substitution aufsteigt, eine Zahl, welche jedoch mit der verschiedenen Wahl der mit g bezeichneten Zahl selbst veränderlich ist. Man darf daher die Frage stellen nach dem kleinsten Werte des Exponenten n, für welchen der gedachte Modulsatz noch Gültigkeit hat. Hurwitz hat in seiner Arbeit (a. a. O.) einige weitere Sätze mitgeteilt, welche nach dieser Seite hin sich verbreiten; hier soll jedoch auf dieselben nur hingewiesen sein.

Im besonderen geht aus dem Satze hervor, daß, wie schon Mertens[1]) bewiesen hat, ein positiver ganzer Exponent h vorhanden ist, so beschaffen, daß jedes Produkt $a_i^h \cdot b^{(1)}$ eine Vielfachsumme der Produkte $a^{(h-1)} \cdot c^{(1)}$ ist. Scheinbar nur ein Teil des gedachten Satzes, erweist sich dieser Ausspruch doch leicht als gleichbedeutend mit dem ganzen Satze. In der Tat, ist h ein solcher Exponent und m die Anzahl aller Koeffizienten a_i, so wird $n = (h-1)m$ eine Zahl sein, wie der gedachte Satz sie behauptet, denn, da jedes Produkt $a^{(n+1)}$ dann gewiß eine der Zahlen a_i mindestens h mal zum Faktor hat, so ist

$$a^{(n+1)} \cdot b^{(1)} = a^{(n+1-h)} \cdot a_i^h b^{(1)},$$

d. i. gleich $a^{(n+1-h)}$mal einer Vielfachsumme der Produkte $a^{(h-1)} \cdot c^{(1)}$ oder gleich einer Vielfachsumme der Größen $a^{(n)} c^{(1)}$.

Der *Mertens*sche Satz enthält denn auch in sich, um schließlich zum Ausgangspunkte der ganzen letzten

1) F. Mertens, über einen algebraischen Satz, Wiener Sitzgsber. 1892.

Betrachtung zurückzukehren, den *Gaußischen* Fundamentalsatz als eine Folgerung. Denn, sind $A(x)$, $B(x)$, $C(x)$ die ganzen, ganzzahligen Funktionen von x und a_i, b_i, c_i ihre Koeffizienten, ist ferner α der größte gemeinsame Teiler aller Koeffizienten a_i, β derjenige aller Koeffizienten b_i, so ist erstens jedes Produkt $a_i^h \cdot \mathfrak{b}^{(1)}$ als Vielfachsumme der Produkte $\mathfrak{a}^{(h-1)} \cdot \mathfrak{c}^{(1)}$ enthalten im Modulus $\alpha^{h-1} \cdot \mathfrak{c}$, wo $\mathfrak{c}$ der endliche Modulus, welcher die Koeffizienten c_i zu Elementen hat, mithin muß, da α^h der größte gemeinsame Teiler aller Zahlen a_i^h ist, ebenfalls $\alpha^h \cdot \mathfrak{b}^{(1)}$ in $\alpha^{h-1} \cdot \mathfrak{c}$, also $\alpha \cdot \mathfrak{b}^{(1)}$ in $\mathfrak{c}$, d. h. jedes Produkt $\alpha \cdot b_k$ und somit auch ihr größter gemeinsamer Teiler $\alpha \cdot \beta$ in $\mathfrak{c}$ enthalten, nämlich von der Form

$$u_0 c_0 + u_1 c_1 + \cdots + u_{m+n} \cdot c_{m+n}$$

mit ganzzahligen u_i, also durch den größten gemeinsamen Teiler γ aller Koeffizienten c_i teilbar sein. Da aber auch umgekehrt jede der Zahlen c_i und somit jede in $\mathfrak{c}$ enthaltene Zahl nach der Art, wie sich die Koeffizienten des Produkts $C(x)$ aus denen der Faktoren $A(x)$, $B(x)$ bilden, durch $\alpha \cdot \beta$ teilbar sein muß, so ist auch γ teilbar durch $\alpha \cdot \beta$ und somit γ und $\alpha \cdot \beta$ einander gleich. Das heißt: der größte gemeinsame Teiler der Koeffizienten des Produktes $C(x)$ ist das Produkt aus den größten gemeinsamen Teilern der Koeffizienten der Faktoren; insbesondere also ist das Produkt zweier ursprünglichen Funktionen wieder eine ursprüngliche Funktion, eine Aussage, welche derjenigen des Gaußischen Satzes, wie früher bemerkt worden, äquivalent ist.

7. Der allgemeine Funktionensatz der Nr. 3, für welchen wir nunmehr verschiedene Beweise gegeben haben, hat sich in der ihm von Hurwitz gegebenen speziellen Fassung, wie dort gezeigt, als ein Mittel erwiesen, den fundamentalen Satz zu begründen, daß es für jedes Ideal $\mathfrak{j}$ eines Körpers ein anderes Ideal gebe der Art, daß beider Produkt ein Hauptideal sei. Im wesentlichen sind aber die gegebenen Beweise des Funktionensatzes aus gewissen Sätzen entsprungen, welche für algebraische Zahlen gelten, und mit Recht hat daher Dedekind (a. a. O.) es als eine Abweichung vom geraden und natürlichen Wege betrachtet, zuvörderst jenen Satz und dann

erst mittels desselben den die Ideale betreffenden Zahlensatz herzuleiten. Durch anhaltende, diesem Gegenstande gewidmete Bemühungen ist es ihm endlich gelungen, den Idealsatz mit Vermeidung des Funktionensatzes zu gewinnen. Erinnern wir uns dazu, daß der einfache Fall des letzteren, durch dessen wiederholte Anwendung er in seiner Allgemeinheit bewiesen wurde (s. Nr. 4), die Deutung eines rein arithmetischen Resultates war, dem wir dort noch eine zweite Fassung in Gestalt eines Modulsatzes gaben. Versuchen wir zunächst, auch diesen zu verallgemeinern, indem wir ihn ganz allgemein aussprechen, wie folgt:

Jeder n-gliedrige Modulus $\mathfrak{m}$, dessen Elemente algebraische Zahlen sind, kann durch Multiplikation mit einem von Null verschiedenen Modulus $\mathfrak{n}$, dessen Zahlen aus denen von $\mathfrak{m}$ rational gebildet sind, in einen Modulus $\mathfrak{m}\cdot\mathfrak{n}$ verwandelt werden, welcher nur ganze algebraische Zahlen, darunter den Modulus $\mathfrak{z}$, enthält.

Für eingliedrige Moduln $\mathfrak{m} = [\alpha]$ ist der Satz unmittelbar einleuchtend, nämlich $\mathfrak{n} = [\alpha^{-1}]$ ein Modulus der gedachten Beschaffenheit, da offenbar

$$\mathfrak{m}\cdot\mathfrak{n} = [\alpha]\cdot[\alpha^{-1}] = \mathfrak{z}$$

ist. Für zweigliedrige Moduln haben wir den Satz bereits in Nr. 4 festgestellt. Durch eine einfache Induktion läßt sich hieraus der allgemeine Satz erhalten. An der angeführten Stelle vollzieht Dedekind diese Induktion auf rechnerischem Wege; hier benutzen wir, der anderen Methode uns anschließend, die er für dieselbe in Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl., p. 530 verwendet hat, den allgemeinen Modulsatz (9) des zweiten Kapitels, nach welchem für drei beliebige Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ die Beziehung stattfindet:

$$(51)\qquad (\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b}) = (\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a})(\mathfrak{a}+\mathfrak{b}).$$

Nehmen wir nämlich an, der fragliche Satz sei bereits bewiesen für alle aus algebraischen Zahlen bestehenden Moduln von einer Gliederzahl, welche kleiner als n ist, so brauchen wir nur zu zeigen, daß er auch noch für n-gliedrige Moduln dieser Art stattfindet; man darf dabei $n \geqq 3$ voraussetzen.

Sei also $\mathfrak{m}$ ein solcher; indem wir seine n Basiszahlen in drei Gruppen verteilen in der Weise, daß jede von ihnen wenigstens ein Glied enthält, und die aus diesen Gruppen gebildeten endlichen Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ nennen, sodaß

$$\mathfrak{m} = \mathfrak{a} + \mathfrak{b} + \mathfrak{c} \tag{52}$$

wird, erhalten wir in den Moduln $\mathfrak{b} + \mathfrak{c}$, $\mathfrak{c} + \mathfrak{a}$, $\mathfrak{a} + \mathfrak{b}$ drei, weniger als n-gliedrige, aber von Null verschiedene Moduln, deren Zahlen, weil in $\mathfrak{m}$ enthalten, algebraische Zahlen sind, und folglich gibt es nach der Voraussetzung drei aus ihren entsprechenden Zahlen d. i. aus Zahlen von $\mathfrak{m}$ rational gebildete Moduln $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$ von der Beschaffenheit, daß die Produkte

$$(\mathfrak{b} + \mathfrak{c})\mathfrak{a}', \quad (\mathfrak{c} + \mathfrak{a})\mathfrak{b}', \quad (\mathfrak{a} + \mathfrak{b})\mathfrak{c}'$$

Moduln sind, welche $\mathfrak{z}$ und überhaupt nur ganze algebraische Zahlen in sich enthalten. Demnach gilt von ihrem Produkte

$$(\mathfrak{b} + \mathfrak{c})(\mathfrak{c} + \mathfrak{a})(\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{a}'\mathfrak{b}'\mathfrak{c}',$$

d. i. nach (51) und (52) von dem Produkte

$$\mathfrak{m} \cdot (\mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b})\mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$$

das Gleiche, und folglich ist der Modulus

$$\mathfrak{n} = (\mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b})\mathfrak{a}'\mathfrak{b}'\mathfrak{c}',$$

dessen Zahlen ersichtlich ebenfalls aus denen von $\mathfrak{m}$ auf rationale Weise gebildet sind, ein Modulus von der im Satze behaupteten Beschaffenheit. Dieser Satz ist also bewiesen.

Auf Grund desselben gelangt man nun einfach zum Ziele durch nachfolgende Betrachtung. Ist $\mathfrak{j}$ ein Ideal des Körpers $K(\mathsf{A}; R)$ vom Grade n, so gibt es dem Satze zufolge einen aus den Zahlen von $\mathfrak{j}$, d. i. aus Zahlen desselben Körpers gebildeten Modulus $\mathfrak{m}$ von der Beschaffenheit, daß der Modulus $\mathfrak{j} \cdot \mathfrak{m}$ den Modulus $\mathfrak{z}$ und überhaupt nur ganze Zahlen des Körpers oder Zahlen in $\mathfrak{g}$ enthält; demgemäß bestehen die Beziehungen

$$\mathfrak{z} \succ \mathfrak{j} \cdot \mathfrak{m} \succ \mathfrak{g},$$

aus deren erster durch Multiplikation mit $\mathfrak{g}$ in Rücksicht auf die Gleichungen $\mathfrak{z}\mathfrak{g} = \mathfrak{g}$, $\mathfrak{j}\mathfrak{g} = \mathfrak{j}$ die folgende

$$\mathfrak{g} \succ \mathfrak{j} \cdot \mathfrak{m}$$

und nun durch Verbindung mit der zweiten jener Beziehungen

die *Gleichheit*

$$(53)\qquad \mathfrak{j}\cdot\mathfrak{m}=\mathfrak{g}$$

hervorgeht. *Nun ist die Ordnung* $\mathfrak{j}^0$ *eines jeden Ideales* $\mathfrak{j}$ *gleich* $\mathfrak{g}$; denn diese Ordnung ist die Gesamtheit aller Zahlen α, für welche $\mathfrak{j}\cdot\alpha \succ \mathfrak{j}$ ist, eine Gesamtheit, zu welcher nach der Definition eines Ideales alle Zahlen in $\mathfrak{g}$ gehören, während $\mathfrak{j}^0$ nach Kap. 4, Nr. 6 auch nur solche Zahlen enthält. Daher läßt sich die Gleichheit (53) auch durch die folgende:

$$(54)\qquad \mathfrak{j}\cdot\mathfrak{m}=\mathfrak{j}^0$$

ersetzen.

Ist ferner $\mathfrak{j}'=\frac{\mathfrak{j}^0}{\mathfrak{j}}$, nämlich gleich der Gesamtheit aller Zahlen α, für welche $\mathfrak{j}\alpha \succ \mathfrak{j}^0$ ist, so zeigt sich leicht, daß $\mathfrak{j}^0\cdot\mathfrak{j}'=\mathfrak{j}'$ ist; denn erstens ist, da $\mathfrak{j}^0$ als Ordnung eines Modulus die Zahl 1 enthält,

$$(55)\qquad \mathfrak{j}' \succ \mathfrak{j}^0\mathfrak{j}';$$

andererseits folgt aus der für $\mathfrak{j}'$ bestehenden Beziehung

$$(56)\qquad \mathfrak{j}\mathfrak{j}' \succ \mathfrak{j}^0$$

durch Multiplikation mit $\mathfrak{j}^0$ und mit Rücksicht auf die Gleichheit $\mathfrak{j}^0\mathfrak{j}^0=\mathfrak{j}^0$ die Beziehung $\mathfrak{j}\cdot\mathfrak{j}^0\mathfrak{j}' \succ \mathfrak{j}^0$, welche lehrt, daß die Zahlen in $\mathfrak{j}^0\mathfrak{j}'$ zu den zuvor definierten Zahlen α gehören, d. h. daß

$$(57)\qquad \mathfrak{j}^0\mathfrak{j}' \succ \mathfrak{j}'$$

ist. Verbunden mit (55) ergibt sich hieraus die behauptete Gleichheit

$$(58)\qquad \mathfrak{j}^0\mathfrak{j}'=\mathfrak{j}'.$$

Nunmehr folgert man einerseits aus (54) durch Multiplikation mit $\mathfrak{j}^0$ die Gleichung

$$\mathfrak{j}\cdot\mathfrak{j}^0\mathfrak{m}=\mathfrak{j}^0,$$

derzufolge $\mathfrak{j}^0\mathfrak{m} \succ \mathfrak{j}'$ ist, andererseits aus (56) durch Multiplikation mit $\mathfrak{m}$ und Beachtung der Gleichungen (54) und (58) die Beziehung $\mathfrak{j}' \succ \mathfrak{j}^0\mathfrak{m}$, sodaß man endlich findet

$$\mathfrak{j}'=\mathfrak{j}^0\mathfrak{m}$$

und, indem man diese Gleichung mit $\mathfrak{j}$ multipliziert und (54) in Betracht zieht, die Gleichung

$$\mathfrak{j}\mathfrak{j}' = \mathfrak{j}^0,$$

der auch die Gestalt gegeben werden kann

$$\mathfrak{j}\mathfrak{j}' = \mathfrak{g}. \tag{59}$$

Dies vorausgeschickt, seien $\alpha_1, \alpha_2, \cdots, \alpha_n$ die Basiszahlen des Ideals $\mathfrak{j}$ und

$$\gamma = \alpha_1 \alpha_2 \cdots \alpha_n.$$

Nach Kap. 4, Nr. 6 besteht der Modulus $\mathfrak{j}'$ aus denjenigen Zahlen, welche den Moduln

$$\mathfrak{j}^0 \cdot \alpha_1^{-1},\ \mathfrak{j}^0 \cdot \alpha_2^{-1},\ \cdots,\ \mathfrak{j}^0 \cdot \alpha_n^{-1}$$

gemeinsam sind, ebenso also der Modulus $\mathfrak{j}' \cdot \gamma$ aus den Zahlen, welche allen Moduln

$$\mathfrak{j}^0 \cdot \frac{\gamma}{\alpha_i}$$
$$(\text{für } i = 1, 2, \cdots, n)$$

gemeinsam, jedenfalls also Zahlen in $\mathfrak{g}$ sind. Der Modulus $\mathfrak{j}'' = \mathfrak{j}' \cdot \gamma$ ist also ein Modulus ganzer Zahlen des Körpers, der die Bedingung erfüllt

$$\mathfrak{j}'' \cdot \mathfrak{g} = \mathfrak{j}'' \cdot \mathfrak{j}^0 = \mathfrak{j}'\mathfrak{j}^0 \cdot \gamma = \mathfrak{j}' \cdot \gamma = \mathfrak{j}'';$$

der Modulus $\mathfrak{j}''$ ist also ein Ideal. Aus der Gleichung (59) aber folgt durch Multiplikation mit γ die andere

$$\mathfrak{j} \cdot \mathfrak{j}'' = \mathfrak{g}\gamma,$$

also gibt es, wie der fundamentale Satz, den wir zu beweisen haben, behauptet, für jedes Ideal $\mathfrak{j}$ ein anderes, welches, mit jenem multipliziert, ein Hauptideal hervorbringt.

8. Der letztmitgeteilte Dedekindsche Beweis dieses Fundamentalsatzes darf als der sachgemäßeste bezeichnet werden, weil er unmittelbar und ausschließlich aus dem Ideenkreise geschöpft ist, welchem der Satz selbst zugehört. Indessen kommt einem andern Beweise, den man Hurwitz verdankt[1]),

---

1) A. Hurwitz, Zur Theorie der algebraischen Zahlen, Göttinger Nachr. 1895, Heft 3.

noch der Vorzug zu, daß er, ohne auch seinerseits jenen Ideenkreis zu verlassen oder größerer Vorbereitungen zu bedürfen, sich nur eines Satzes bedient, der als eine Verallgemeinerung des bekannten Euclidischen Verfahrens zur Aufsuchung des größten gemeinsamen Teilers zweier rationalen ganzen Zahlen betrachtet werden darf, und so die Lehre von der Teilbarkeit der algebraischen ganzen Zahlen auf eine ganz analoge Grundlage stellt, wie diejenige, auf welcher sie für die rationalen ganzen Zahlen beruht. Zudem basiert jener Satz auf der ganz einfachen Tatsache, daß, wenn m Zahlen in weniger als m Intervalle verteilt werden, notwendig in wenigstens eins dieser Intervalle mehr als eine Zahl hineinfallen muß, derselben Tatsache, aus welcher, wie später genauer dargestellt werden wird, Dirichlet seine allgemeine Theorie der Einheiten entwickelt hat.

Der genannte Hurwitzsche Grundsatz besagt Folgendes:

Ist ζ eine beliebige Zahl des Körpers $K(\mathsf{A}; R)$ vom Grade n, so läßt sich eine ganze Zahl μ dieses Körpers und eine positive rationale ganze Zahl h so bestimmen, daß die Norm der Zahl $h\zeta - \mu$ absolut kleiner als 1 ist; dabei ist h nicht größer als eine positive ganze Zahl m, welche, von ζ unabhängig, nur vom Körper selbst bestimmt ist. Um dies zu beweisen, verstehe man unter den Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ irgend eine ganzzahlige Basis des Körpers, sodaß jede Zahl ζ desselben in der Form

$$\zeta = r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$$

mit rationalen Koeffizienten r_i dargestellt werden kann. Dann sei k eine zunächst unbestimmte positive ganze Zahl und man bestimme für jeden der $k^n + 1$ Werte

$$i = 0, 1, 2, 3, \cdots, k^n$$

die ganze Zahl

$$\mu_i = \varrho_1\omega_1 + \varrho_2\omega_2 + \cdots + \varrho_n\omega_n$$

des Körpers mit ganzzahligen ϱ_i so, daß die Koeffizienten in der Zahl

$$(60)\quad i\zeta - \mu_i = (ir_1 - \varrho_1)\omega_1 + (ir_2 - \varrho_2)\omega_2 + \cdots + (ir_n - \varrho_n)\omega_n$$

sämtlich zwischen 0 inklusive und 1 exklusive enthalten sind;

auf diese Weise erhält man $k^n + 1$ Zahlen. Zerlegt man also das Intervall von 0 bis 1 in die k Teilintervalle

$$0 \cdots \frac{1}{k}, \ \frac{1}{k} \cdots \frac{2}{k}, \ \cdots, \ \frac{k-1}{k} \cdots 1,$$

indem man zu jedem einzelnen Teilintervalle seine untere Grenze, die obere Grenze aber zum folgenden rechnet, so gibt es, da jeder der n Koeffizienten in (60) jedem dieser Teilintervalle zugehören kann, im ganzen k^n Möglichkeiten, wie die Koeffizienten der Zahlen (60) sich auf die k Intervalle verteilen. Daher muß diese Verteilung wenigstens für zwei der $k^n + 1$ Zahlen (60) die gleiche sein, und wenn demnach

$$(61) \qquad h\zeta - \mu = \delta_1 \omega_1 + \delta_2 \omega_2 + \cdots + \delta_n \omega_n$$

die Differenz der letzteren zwei Zahlen bedeutet, so müssen die sämtlichen Koeffizienten δ_i derselben numerisch kleiner als $\frac{1}{k}$ sein, während h eine der Zahlen 1, 2, 3, $\cdots$, k^n bedeutet. Aus (61) folgt daher, daß der absolute Betrag von $h\zeta - \mu$ gewiß nicht größer ist, als $\frac{1}{k}$ mal der Summe der absoluten Beträge der Basiszahlen ω_i, welche ω heiße. Bildet man aber die zu $h\zeta - \mu$ konjugierten Zahlen, so gilt für ihre absoluten Beträge Entsprechendes, und somit wird endlich der absolute Betrag der Norm $N(h\zeta - \mu)$ kleiner sein als eine Zahl Ω, welche nur durch den Körper selbst bestimmt ist, multipliziert mit $\frac{1}{k^n}$. Wird daher nun die bisher beliebige Zahl $k > \sqrt[n]{\Omega}$, etwa als die zunächst über $\sqrt[n]{\Omega}$ liegende ganze Zahl gedacht, so wird die Norm von $h\zeta - \mu$ absolut kleiner als Eins und der behauptete Satz mithin richtig sein, wenn $m = k^n$ gewählt wird.

Dies nun vorausgeschickt, sei $\mathfrak{j}$ ein beliebig gegebenes Ideal des Körpers und α irgend eine von Null verschiedene Zahl in $\mathfrak{j}$; wir setzen zudem voraus, daß ihre Norm, die bekanntlich eine von Null verschiedene rationale ganze Zahl ist, möglichst klein sei, sodaß in $\mathfrak{j}$ keine andere von Null verschiedene Zahl vorhanden ist, deren Norm absolut kleiner ist als $N(\alpha)$. Ist dann α' irgend eine andere in $\mathfrak{j}$ enthaltene Zahl,

so ergibt die Anwendung des Hilfssatzes auf die Zahl $\zeta = \frac{\alpha'}{\alpha}$ das Resultat, daß es eine Zahl $h\alpha' - \mu\alpha$ gibt, deren Norm absolut kleiner ist als $N(\alpha)$. Diese ganze, dem Ideale $\mathfrak{j}$ angehörige Zahl muß dann dem Gesagten zufolge gleich Null, also

$$h\alpha' = \mu\alpha$$

d. i. $h\alpha'$ durch α teilbar sein. Da h aber eine Zahl der Reihe $1, 2, 3, \cdots, m$ bezeichnet, so muß dann auch, $M = 1\cdot 2\cdot 3\cdots m$ gesetzt,

$$M\alpha',$$

nämlich jede Zahl des Ideals $M\mathfrak{j}$ durch α teilbar sein. Diese, sämtlich durch α teilbaren Zahlen bilden aber offenbar ein Ideal von der Gestalt $\alpha\cdot\mathfrak{j}'$, wo auch $\mathfrak{j}'$ ein Ideal des Körpers bedeutet, und man erhält daher die Gleichheit

$$M\cdot\mathfrak{j} = \alpha\cdot\mathfrak{j}', \tag{62}$$

welche die Äquivalenz der beiden Ideale $\mathfrak{j}, \mathfrak{j}'$ aussagt. Nun kommt im Ideale $M\cdot\mathfrak{j}$ auch die Zahl $M\cdot\alpha$ vor, der Gleichung zufolge also die Zahl M im Ideale $\mathfrak{j}'$. Da es aber (nach Nr. 2) nur eine endliche Anzahl Ideale, umsomehr also auch nur eine endliche Anzahl nicht äquivalenter Ideale gibt, in denen eine gegebene rationale ganze Zahl enthalten ist, lehrt die Gleichung (62) den Satz:

Daß jedes beliebig gegebene Ideal $\mathfrak{j}$ stets einem von einer endlichen Anzahl von nicht äquivalenten Idealen, welche durch die nur vom Körper abhängige ganze Zahl M fest bestimmt sind, äquivalent ist.

Diese, die Zahl M enthaltenden Ideale repräsentieren also die verschiedenen Klassen untereinander äquivalenter Ideale des Körpers, und demnach ist die Anzahl der Idealklassen endlich.

Bezeichnet jetzt h diese endliche Anzahl, so ergibt sich sogleich die Folgerung, daß unter den $h+1$ Idealen

$$\mathfrak{j}, \mathfrak{j}^2, \mathfrak{j}^3, \cdots, \mathfrak{j}^{h+1}$$

mindestens zwei einander äquivalent sein müssen. Sind dies etwa $\mathfrak{j}^r, \mathfrak{j}^s$, wo $s > r$, so besteht eine Gleichung von der Form

$$\gamma' \cdot \mathfrak{j}^r = \gamma'' \cdot \mathfrak{j}^s,$$

wo γ', γ'' zwei ganze Zahlen des Körpers bedeuten und welche, wenn $\gamma = \frac{\gamma'}{\gamma''}$ gesetzt wird, auch so geschrieben werden kann:

$$(63) \qquad \gamma \cdot \mathfrak{j}^r = \mathfrak{j}^r \cdot \mathfrak{j}^{s-r}.$$

Nun bezeichne man mit

$$\alpha_1, \alpha_2, \cdots, \alpha_n; \quad \beta_1, \beta_2, \cdots, \beta_n$$

die Basiszahlen bzw. des Ideales $\mathfrak{j}^r$ und des Ideales $\mathfrak{j}^{s-r}$. Dann folgert man aus (63) zunächst, daß die im Ideale $\gamma \cdot \mathfrak{j}^r$ enthaltenen Zahlen

$$\gamma\alpha_1, \gamma\alpha_2, \cdots, \gamma\alpha_n$$

sämtlich homogene lineare Ausdrücke der Größen $\alpha_1, \alpha_2, \cdots, \alpha_n$ sind mit Koeffizienten, welche dem Ideale $\mathfrak{j}^{s-r}$ angehörig also ganze algebraische Zahlen sind, und hieraus folgt in bekannter Weise, daß die dem Körper angehörige Zahl γ eine ganze, d. i. eine Zahl in $\mathfrak{g}$ ist. Andererseits sind der Gleichung (63) zufolge die im Ideale zu ihrer Rechten enthaltenen Zahlen

$$\beta_i\alpha_1, \beta_i\alpha_2, \cdots, \beta_i\alpha_n$$
$$(i = 1, 2, \cdots, n)$$

sämtlich homogene lineare Ausdrücke der Größen $\gamma\alpha_1, \gamma\alpha_2, \cdots, \gamma\alpha_n$ mit ganzzahligen Koeffizienten, woraus in derselben Weise folgt, daß jeder der Quotienten $\frac{\beta_i}{\gamma}$ eine ganze Zahl γ_i des Körpers ist, und daß also

$$\mathfrak{j}^{s-r} = \gamma \cdot \mathfrak{j}'$$

ist, wenn unter $\mathfrak{j}'$ das Ideal mit den Basiszahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ verstanden wird. Demnach nimmt (63) die Gestalt an

$$\mathfrak{j}^r = \mathfrak{j}^r \cdot \mathfrak{j}'$$

und lehrt, daß die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$ homogen und linear durch ebendieselben Zahlen darstellbar sind mit Koeffizienten, welche dem Ideale $\mathfrak{j}'$ angehörig sind; die Elimination dieser Zahlen ergibt eine Gleichung mit ebensolchen Koeffizienten, deren höchster gleich 1 ist, und mit der Wurzel 1; also ist 1 offenbar eine Zahl des Ideals $\mathfrak{j}'$, das Ideal demnach mit $\mathfrak{g}$ identisch und

$$\mathfrak{j}^{s-r} = \mathfrak{g}\gamma.$$

Man erschließt also den Satz: Für jedes Ideal $\mathfrak{j}$ gibt es eine gewisse positive Potenz $\mathfrak{j}^k$, welche ein Hauptideal ist. Wenn nun $k > 1$, so ist $\mathfrak{j}' = \mathfrak{j}^{k-1}$ ein Ideal, mit welchem multipliziert $\mathfrak{j}$ ein Hauptideal wird; für $k = 1$, d. h. wenn $\mathfrak{j}$ selbst ein Hauptideal ist, leistet das Ideal $\mathfrak{j}' = \mathfrak{g}$ nach der Formel $\mathfrak{g}\mathfrak{j} = \mathfrak{j}$ das Gleiche. Somit gibt es immer ein Ideal $\mathfrak{j}'$, welches mit $\mathfrak{j}$ multipliziert ein Hauptideal hervorbringt, und der fundamentale Satz ist aufs neue bewiesen.

9. Wir ziehen aber aus der letzten Betrachtung noch weitere Folgerungen. Ist $\mathfrak{j}^k$ die niedrigste Potenz des Ideals $\mathfrak{j}$, welche ein Hauptideal ist, so erkennt man zunächst leicht, daß k ein Teiler von der Anzahl h der Idealklassen ist. Denn erstens müssen die Potenzen

$$\mathfrak{j},\ \mathfrak{j}^2,\ \mathfrak{j}^3,\ \cdots,\ \mathfrak{j}^k \tag{64}$$

unter einander inäquivalent sein, da aus der Äquivalenz von zweien derselben eine Gleichung von der Form (63) und aus ihr eine Potenz $\mathfrak{j}^{k'}$, deren Exponent $k' < k$ wäre, als ein Hauptideal hervorgehen würde. Wäre nun $k < h$, so gäbe es noch ein Ideal $\mathfrak{j}'$, welches keinem Ideale der Reihe (64) äquivalent wäre. Dann würden die Ideale

$$\mathfrak{j}'\mathfrak{j},\ \mathfrak{j}'\mathfrak{j}^2,\ \mathfrak{j}'\mathfrak{j}^3,\ \cdots,\ \mathfrak{j}'\mathfrak{j}^k \tag{65}$$

sowohl unter sich, als auch mit den Idealen (64) inäquivalent sein; denn aus einer Gleichung

$$\omega' \cdot \mathfrak{j}'\mathfrak{j}^r = \omega'' \cdot \mathfrak{j}'\mathfrak{j}^s$$

erhielte man durch Multiplikation mit einem Ideale $\mathfrak{j}''$, für welches $\mathfrak{j}'\mathfrak{j}''$ ein Hauptideal $\mathfrak{g}\gamma$ wird, die andere:

$$\omega'\gamma \cdot \mathfrak{j}^r = \omega''\gamma \cdot \mathfrak{j}^s,$$

welche die Äquivalenz zweier Ideale der Reihe (64) aussagen würde, gegen das bereits Bewiesene. Desgleichen folgte aus einer Gleichung

$$\omega' \cdot \mathfrak{j}'\mathfrak{j}^r = \omega'' \cdot \mathfrak{j}^s$$

durch Multiplikation mit $\mathfrak{j}^{k-r}$ und in Beachtung des Umstandes, daß $\mathfrak{j}^k$ ein Hauptideal $\mathfrak{g}\gamma$ ist, die andere

$$\omega'\gamma \cdot \mathfrak{j}' = \omega'' \cdot \mathfrak{j}^{k+s-r},$$

aus welcher die Äquivalenz des Ideals $\mathfrak{j}'$ mit einem Ideale der Reihe (64) hervorginge, was gegen die Voraussetzung ist. Hiernach ist h mindestens gleich $2k$. Wenn aber $h > 2k$ ist, so gibt es noch ein Ideal $\mathfrak{j}''$, welches weder mit einem Ideale der Reihe (64) noch einem der Reihe (65) äquivalent ist, und man schließt daraus, daß die k Ideale

$$(66) \qquad \mathfrak{j}''\mathfrak{j},\ \mathfrak{j}''\mathfrak{j}^2,\ \mathfrak{j}''\mathfrak{j}^3,\ \cdots,\ \mathfrak{j}''\mathfrak{j}^k$$

sowohl untereinander als auch mit den Idealen (64) inäquivalent sind; sie sind es aber auch mit den Idealen (65), denn aus einer Gleichung

$$\omega' \cdot \mathfrak{j}'\mathfrak{j}^r = \omega'' \cdot \mathfrak{j}''\mathfrak{j}^s$$

erhielte man durch Multiplikation mit $\mathfrak{j}^{k-s}$ eine Gleichung von der Form

$$\omega' \cdot \mathfrak{j}'\mathfrak{j}^{k'} = \omega''\gamma \cdot \mathfrak{j}'',$$

welche der Annahme, daß $\mathfrak{j}''$ mit keinem der früheren Ideale äquivalent sei, widerspricht. Demnach ist $h \geqq 3k$, usw. Da auf solche Weise die endliche Menge der nicht äquivalenten Ideale erschöpft werden muß, findet sich h als Vielfaches von k, was die Behauptung bestätigt.

Da nun $\mathfrak{j}^k$ ein Hauptideal ist, so folgt hieraus auch $\mathfrak{j}^h$ als ein Hauptideal, oder der Satz: Ist h die Anzahl der nicht äquivalenten Idealklassen, so ist die h^{te} Potenz eines jeden Ideales ein Hauptideal:

$$(67) \qquad \mathfrak{j}^h = \mathfrak{g}\gamma.$$

Ferner gilt der Satz: Aus der Gleichung

$$(68) \qquad \mathfrak{j} \cdot \mathfrak{j}' = \mathfrak{j} \cdot \mathfrak{j}'',$$

in welcher $\mathfrak{j}, \mathfrak{j}', \mathfrak{j}''$ drei Ideale des Körpers bezeichnen, folgt stets die andere:

$$(69) \qquad \mathfrak{j}' = \mathfrak{j}'';$$

denn, ist $\mathfrak{m}$ ein Ideal, für welches $\mathfrak{j} \cdot \mathfrak{m}$ ein Hauptideal $\mathfrak{g}\gamma$ wird, so folgt aus der vorausgesetzten Gleichung durch Multiplikation mit $\mathfrak{m}$ die Beziehung

$$\mathfrak{g}\gamma \cdot \mathfrak{j}' = \mathfrak{g}\gamma \cdot \mathfrak{j}''$$

d. i. $\gamma\mathfrak{j}' = \gamma\mathfrak{j}''$, woraus die behauptete Folgerung fließt. Insbesondere schließt man also aus der Gleichheit

$$\mathfrak{j} \cdot \mathfrak{j}' = \mathfrak{j} = \mathfrak{j} \cdot \mathfrak{g}$$

stets, daß $\mathfrak{j}' = \mathfrak{g}$ ist.

Weil die Klasse, zu welcher das Produkt zweier Ideale gehört, das Produkt der Klassen ist, zu denen diese Ideale gehören, so übertragen sich diese Idealsätze unmittelbar auf die Idealklassen, sodaß man sagen darf:

Zu jeder Idealklasse C gibt es eine andere C' von der Beschaffenheit, daß beider Produkt die Hauptklasse ist, in Zeichen:

$$C \cdot C' = H. \tag{70}$$

Ist demnach für drei Idealklassen A, B, C die Gleichung erfüllt

$$AC = BC,$$

so erschließt man daraus, indem man sie mit C' multipliziert die andere:

$$A \cdot CC' = B \cdot CC',$$

d. h.

$$A \cdot H = B \cdot H$$

oder nach (15) die Gleichheit

$$A = B.$$

Insbesondere folgt hiernach aus der Gleichung

$$AC = C = HC$$

immer $A = H$, die Umkehrung des in der Gleichung (15) ausgesprochenen Satzes. Nun ergibt sich wegen (67) der fernere Satz, daß die h^{te} Potenz jeder Idealklasse der Hauptklasse gleich ist:

$$C^h = H. \tag{71}$$

Verbindet man diese Gleichung mit der Gleichung (70), indem man schreibt

$$C \cdot C^{h-1} = C \cdot C',$$

so erhält man aus den letzten Resultaten

$$C^{h-1} = C', \tag{72}$$

d. h. die Klasse C', welche der Gleichung (70) Genüge tut, ist eine durch diese Beziehung charakterisierte, völlig bestimmte, nämlich gegeben durch die Formel

(72). Sie soll die zu C inverse, reziproke oder entgegengesetzte Klasse heißen.

10. Ferner seien $\alpha_1, \alpha_2, \cdots, \alpha_r$ irgend welche gegebene ganze algebraische Zahlen. Man kann stets einen endlichen Körper $\mathfrak{K}$ bilden, welcher sie sämtlich enthält, z. B. indem man, wie in Kap. 1, Nr. 10 für zwei Körper gezeigt worden ist, allgemeiner die r endlichen Körper

$$K(\alpha_1;\, R),\ K(\alpha_2;\, R),\ \cdots,\ K(\alpha_r;\, R),$$

welche durch die gegebenen Zahlen erzeugt werden, mit einander zusammensetzt. Für diesen Körper $\mathfrak{K}$ sei h die Anzahl seiner Idealklassen und

$$\mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_r\}$$

das in Analogie mit Kap. 4, Formel (20) bestimmte, in $\mathfrak{K}$ enthaltene Ideal. Da wegen (67)

$$\mathfrak{j}^h = \mathfrak{g}\gamma \tag{73}$$

gesetzt werden kann, wo γ eine ganze algebraische Zahl des Körpers $\mathfrak{K}$ bedeutet, und da in $\mathfrak{j}^h$ jede der Potenzen $\alpha_1^h, \alpha_2^h, \cdots, \alpha_r^h$ sich findet, so muß jede von diesen durch γ und demnach jede der Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$ durch die Zahl $\sqrt[h]{\gamma} = \gamma_0$, welche nach Kap. 1, Nr. 3 ebenfalls eine ganze Zahl ist, teilbar sein; γ_0 ist also ein gemeinsamer Teiler der gegebenen Zahlen und daher wird auch jeder Teiler von γ_0 ein gemeinsamer Teiler von ihnen sein. Umgekehrt aber ergibt sich aus (73) die Zahl γ, weil in $\mathfrak{j}^h$ enthalten, gleich einer homogenen Funktion h^{ter} Dimension von den Größen $\alpha_1, \alpha_2, \cdots, \alpha_r$ mit algebraisch ganzen, dem Körper angehörigen Koeffizienten, eine Beziehung, der man die Form geben kann:

$$\gamma = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_r\beta_r, \tag{74}$$

wenn man unter $\beta_1, \beta_2, \cdots, \beta_r$ homogene Funktionen $h-1^{\text{ter}}$ Dimension von den α_i versteht mit Koeffizienten, welche ganze Zahlen in $\mathfrak{K}$ sind. Ist also δ ein gemeinsamer Teiler von $\alpha_1, \alpha_2, \cdots, \alpha_r$, so wird δ^h aufgehen in $\gamma = \gamma_0^h$, mithin δ in γ_0, und somit jeder gemeinsame Teiler jener Zahlen auch umgekehrt ein Teiler von γ_0 sein. Daher stimmen die den Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$ gemeinsamen Teiler völlig überein mit den

sämtlichen Teilern der Zahl γ_0, welche man wegen (74) darstellen kann in der Form

$$\gamma_0 = \alpha_1\gamma_1 + \alpha_2\gamma_2 + \cdots + \alpha_r\gamma_r, \tag{75}$$

worin $\gamma_1, \gamma_2, \cdots, \gamma_r$ ganze Zahlen bedeuten, die jedoch, so wenig wie die Zahl γ_0, dem Körper $\mathfrak{K}$ anzugehören brauchen. Für irgend welche gegebene ganze algebraische Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$ gibt es also stets eine ganze Zahl γ_0 von der Form (75) und von der Beschaffenheit, daß ihre sämtlichen Teiler völlig identisch sind mit den, den gegebenen Zahlen gemeinsamen Teilern. In Analogie mit der gewöhnlichen Zahlentheorie wird diese Zahl γ_0 der größte gemeinsame Teiler der gegebenen Zahlen genannt. Ist sie eine Einheit, so heißen die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$, welche dann auch nur Einheiten zu gemeinsamen Teilern haben können, Zahlen ohne gemeinsamen Teiler und werden, falls ihrer nur zwei vorhanden sind, relativ prim genannt. Der Gleichung (75) darf in letzterem Falle die einfachere Form gegeben werden:

$$\alpha_1\gamma_1 + \alpha_2\gamma_2 = 1. \tag{76}$$

Zwei relativ prime Zahlen α_1, α_2 sind also gleichermaßen durch den Umstand charakterisiert, daß sie keine anderen gemeinsamen Teiler besitzen als Einheiten (deren jede selbstverständlich ihnen beiden gemeinsam ist), wie durch die Auflösbarkeit der Gleichung (76) in ganzen algebraischen Zahlen γ_1, γ_2.

Hieraus fließen für relativ prime algebraische Zahlen ganz analoge Sätze, wie sie für solche rationale Zahlen Geltung haben. Z. B.:

Sind α_1, α_2 relativ prim und ist das Produkt $\alpha_1\beta_1$, dessen zweiter Faktor ebenfalls eine ganze Zahl ist, teilbar durch α_2, so muß β_1 durch α_2 teilbar sein. Denn aus (76) folgt

$$\alpha_1\beta_1 \cdot \gamma_1 + \alpha_2 \cdot \gamma_2\beta_1 = \beta_1,$$

eine Gleichung, derzufolge jeder gemeinsame Teiler von $\alpha_1\beta_1$ und α_2 notwendig auch in β_1 aufgeht.

Sooft daher sowohl α_1 als auch β_1 relativ prim ist zu α_2, muß es auch ihr Produkt sein, denn dann haben

β_1, α_2 keine von Einheiten verschiedene gemeinsame Teiler. Hieraus folgt allgemeiner: Ist jede der Zahlen $\alpha_1, \alpha_2, \alpha_3, \cdots$ relativ prim zu jeder der Zahlen $\beta_1, \beta_2, \cdots$, so ist auch das Produkt von beliebigen der ersteren relativ prim zum Produkte von beliebigen der letzteren Zahlen. Insbesondere sind die Potenzen α^r, β^s mit positiven ganzen Exponenten relativ prim, wenn α, β es sind.

Ist ferner eine Zahl γ teilbar durch jede der zwei relativ primen Zahlen α_1, α_2, so ist sie auch teilbar durch ihr Produkt. Denn, setzt man $\gamma = \alpha_1\beta_1$, so muß, da $\alpha_1\beta_1$ teilbar sein soll durch α_2, zu welcher Zahl α_1 relativ prim ist, die ganze Zahl β_1 teilbar sein durch α_2, etwa $\beta_1 = \alpha_2\delta$, mithin $\gamma = \alpha_1\alpha_2 \cdot \delta$, wo δ eine ganze Zahl.

Wenngleich die Analogie mit der gewöhnlichen Zahlentheorie, wie diese Sätze zeigen, sich weit auch in die Theorie der, ohne jede Beschränkung gedachten, ganzen algebraischen Zahlen hinein erhält, so läßt sie doch, wie früher bemerkt ist, im Stich, sobald man nach den unzerlegbaren Teilern einer Zahl forscht, was uns veranlaßte, uns auf die Betrachtung der Zahlen eines endlichen Körpers zu beschränken; und wir kehren daher von dieser Abschweifung, zu der wir zuletzt uns führen ließen, jetzt wieder zu jenen Zahlen ausschließlich zurück.

11. Durch den nunmehr verschiedentlich bewiesenen Fundamentalsatz, für welchen an späterer Stelle (Kap. 12, Nr. 2 und 3) noch ein weiterer, von Hilbert herrührender Beweis gegeben werden soll, ist nach Nr. 3 zugleich festgestellt, daß, wenn ein Ideal $\mathfrak{c}$ in einem Ideale $\mathfrak{a}$ enthalten oder wenn, unserer Ausdrucksweise gemäß, $\mathfrak{a}$ ein Teiler von $\mathfrak{c}$ ist, eine Gleichung $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ angesetzt werden kann, in welcher auch $\mathfrak{b}$ ein Ideal ist, daß mithin $\mathfrak{a}$ dann auch ein Faktor von $\mathfrak{c}$ ist. Da das Umgekehrte nach Nr. 1 ebenfalls stattfindet, so ergibt sich die völlige Identität des Begriffs eines *Teilers* mit demjenigen eines *Faktors* eines Ideales. Hiermit ist aber die Grundlage gewonnen für den Nachweis, daß die Gesetze, welche die Teilbarkeit der Ideale eines endlichen Körpers $K(\mathsf{A}; R)$ beherrschen, völlig übereinstimmen mit denjenigen der gewöhnlichen Zahlentheorie, daß insbesondere jedes Ideal

auf ganz entsprechende Weise eindeutig in *Primideale* zerlegt werden kann, wie die natürlichen Zahlen in *Primfaktoren*.

Wir entwickeln zunächst eine Reihe von Teilbarkeitssätzen, zu deren Begründung dieser Begriff des Primideales noch nicht erforderlich ist.

Ein Ideal $\mathfrak{d}$ heißt ein gemeinsamer Teiler mehrerer Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$, wenn jedes von diesen in $\mathfrak{d}$ enthalten ist:

$$\mathfrak{a} \succ \mathfrak{d}, \quad \mathfrak{b} \succ \mathfrak{d}, \quad \mathfrak{c} \succ \mathfrak{d}, \cdots;$$

nach Kap. 2, Nr. 1 ist $\mathfrak{d}$ dann auch ein Teiler des größten gemeinsamen Teilers von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$:

$$\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots \succ \mathfrak{d}. \tag{77}$$

Nun ist das Ideal $\mathfrak{g}$ Teiler eines jeden Ideales $\mathfrak{j}$, da $\mathfrak{j}$ in $\mathfrak{g}$ enthalten ist. Haben aber mehrere Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ außer diesem selbstverständlichen Teiler keinen andern Idealteiler gemeinsam, so sollen sie *Ideale ohne gemeinsamen Teiler* und, wenn ihrer nur zwei vorhanden sind, *relativ prime Ideale* genannt werden. Dann kann ihr größter gemeinsamer Teiler $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots$ auch nur gleich $\mathfrak{g}$ sein, und umgekehrt, wenn dies ist, so erfüllt wegen (77) jeder gemeinsame Idealteiler $\mathfrak{d}$ von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ die Bedingung $\mathfrak{g} \succ \mathfrak{d}$, während auch $\mathfrak{d} \succ \mathfrak{g}$ ist, mithin ist $\mathfrak{d} = \mathfrak{g}$ und $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ haben keinen Teiler gemeinsam außer $\mathfrak{g}$. *Demnach sind Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ ohne gemeinsamen Teiler durch die Gleichung*

$$\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots = \mathfrak{g}, \tag{78}$$

insbesondere zwei relativ prime Ideale $\mathfrak{a}, \mathfrak{b}$ durch die Gleichung

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{g} \tag{78a}$$

charakterisiert.

Sei für beliebig viel gegebene Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ ihr größter gemeinsamer Teiler $\mathfrak{d}$, ihr kleinstes gemeinsames Vielfache $\mathfrak{m}$.

Alsdann gibt es *erstens* Ideale $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \cdots$, für welche die Gleichungen bestehen:

$$\mathfrak{a} = \mathfrak{d}\mathfrak{a}', \quad \mathfrak{b} = \mathfrak{d}\mathfrak{b}', \quad \mathfrak{c} = \mathfrak{d}\mathfrak{c}', \cdots, \tag{79}$$

aus denen nach Kap. 2, Formel (8)

$$\mathfrak{a} + \mathfrak{b} + \mathfrak{c} + \cdots = \mathfrak{d}(\mathfrak{a}' + \mathfrak{b}' + \mathfrak{c}' + \cdots), \tag{80}$$

d. h., weil die linke Seite dieser Gleichung mit $\mathfrak{d}$ identisch ist, die Gleichung

$$\mathfrak{d} = \mathfrak{d} \cdot (\mathfrak{a}' + \mathfrak{b}' + \mathfrak{c}' + \cdots),$$

also

$$\mathfrak{a}' + \mathfrak{b}' + \mathfrak{c}' + \cdots = \mathfrak{g} \tag{81}$$

hervorgeht. Erfüllen umgekehrt die in den Gleichungen (79) auftretenden Ideale $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \cdots$ diese Bedingung, so ergibt sich aus (80) $\mathfrak{d}$ als der größte gemeinsame Teiler von $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$. Ist also $\mathfrak{d}$ größter gemeinsamer Teiler der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$, so sind die Ideale $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \cdots$ in den Formeln (79) Ideale ohne gemeinsamen Teiler, und umgekehrt.

Zweitens darf man, da $\mathfrak{m}$ in jedem der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ enthalten ist,

$$\mathfrak{m} = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 = \cdots \tag{82}$$

setzen, wo $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \cdots$ Ideale bedeuten. Man bezeichne mit $\mathfrak{d}$ den größten gemeinsamen Teiler dieser Ideale und mit $\mathfrak{d}'$ (s. Nr. 7) den Modulus $\frac{\mathfrak{d}^0}{\mathfrak{d}}$, für welchen (Formel (59))

$$\mathfrak{d} \cdot \mathfrak{d}' = \mathfrak{g} \tag{83}$$

ist. Setzt man

$$\mathfrak{a}_1 = \mathfrak{d}\mathfrak{a}', \quad \mathfrak{b}_1 = \mathfrak{d}\mathfrak{b}', \quad \mathfrak{c}_1 = \mathfrak{d} \cdot \mathfrak{c}', \cdots,$$

wo auch $\mathfrak{a}', \mathfrak{b}', \mathfrak{c}', \cdots$ Ideale ohne gemeinsamen Teiler bezeichnen, so folgt aus (82) mit Rücksicht auf (83)

$$\mathfrak{m}\mathfrak{d}' = \mathfrak{a}\mathfrak{a}' = \mathfrak{b}\mathfrak{b}' = \mathfrak{c}\mathfrak{c}' = \cdots,$$

folglich $\mathfrak{m}\mathfrak{d}'$ als ein durch jedes der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ teilbares, d. i. in allen diesen Idealen und daher auch in ihrem kleinsten gemeinsamen Vielfachen $\mathfrak{m}$ enthaltenes Ideal, in Zeichen

$$\mathfrak{m}\mathfrak{d}' \succ \mathfrak{m},$$

woraus durch Multiplikation mit $\mathfrak{d}$

$$\mathfrak{m} \succ \mathfrak{m}\mathfrak{d}$$

und, da umgekehrt auch $\mathfrak{m}\mathfrak{d} \succ \mathfrak{m}$ ist, die Gleichheit

$$\mathfrak{m} = \mathfrak{m}\mathfrak{d}$$

und folglich $\mathfrak{d} = \mathfrak{g}$ hervorgeht. Ist also $\mathfrak{m}$ kleinstes gemeinsames Vielfache der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$, so sind die

Ideale $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \cdots$ in den Formeln (82) Ideale ohne gemeinsamen Teiler:

$$\mathfrak{a}_1 + \mathfrak{b}_1 + \mathfrak{c}_1 + \cdots = \mathfrak{g}. \tag{84}$$

Ist $\mathfrak{d}$ der größte gemeinsame Teiler, $\mathfrak{m}$ das kleinste gemeinsame Vielfache zweier Ideale $\mathfrak{a}, \mathfrak{b}$, so ist immer

$$\mathfrak{m} \cdot \mathfrak{d} = \mathfrak{a}\mathfrak{b}. \tag{85}$$

Denn, setzt man $\mathfrak{d} = \mathfrak{a} + \mathfrak{b}$ und $\mathfrak{m} = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1$, wo also $\mathfrak{a}_1 + \mathfrak{b}_1 = \mathfrak{g}$ ist, so folgt

$$\mathfrak{m} \cdot \mathfrak{d} = (\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{m} = \mathfrak{a}\mathfrak{b}(\mathfrak{a}_1 + \mathfrak{b}_1) = \mathfrak{a}\mathfrak{b}.$$

Sind also $\mathfrak{a}, \mathfrak{b}$ zwei relativ prime Ideale, so ist ihr kleinstes gemeinsames Vielfache $\mathfrak{m}$ gleich ihrem Produkte:

$$\mathfrak{m} = \mathfrak{a}\mathfrak{b}, \tag{86}$$

denn in diesem Falle ist $\mathfrak{d} = \mathfrak{g}$.

Unter derselben Voraussetzung ist der größte gemeinsame Teiler von $\mathfrak{a}$ und $\mathfrak{b}\mathfrak{c}$, wo $\mathfrak{c}$ ein beliebiges Ideal ist, gleich dem größten gemeinsamen Teiler von $\mathfrak{a}$ und $\mathfrak{c}$; denn aus $\mathfrak{a} + \mathfrak{b} = \mathfrak{g}$ folgt $\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c} = \mathfrak{c}$; da nun $\mathfrak{a}\mathfrak{c} \succ \mathfrak{a}$ ist, folgt (Kap. 2, Nr. 1) $\mathfrak{a}\mathfrak{c} + \mathfrak{a} = \mathfrak{a}$, also aus der vorhergehenden Gleichung

$$\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c}, \tag{87}$$

eine Beziehung, in welcher die Behauptung des Satzes zum Ausdrucke kommt.

Ist demnach das Ideal $\mathfrak{a}$ relativ prim sowohl zum Ideale $\mathfrak{b}$, wie zum Ideale $\mathfrak{c}$, so ist es auch relativ prim zu ihrem Produkte $\mathfrak{b}\mathfrak{c}$; denn in diesem Falle ist

$$\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a} + \mathfrak{c} = \mathfrak{g},$$

was die Aussage erhärtet. Durch wiederholte Anwendung dieses besonderen Satzes erhält man sogleich den allgemeineren: Sind $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \cdots$ beliebig viel Ideale, deren jedes zu jedem der beliebig vielen Ideale $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_2, \cdots$ relativ prim ist, so ist auch das Produkt der ersteren relativ prim zum Produkte der letzteren. Z. B. ist jede positive ganze Potenz $\mathfrak{a}^r$ relativ prim zu jeder solchen Potenz $\mathfrak{b}^s$, wenn $\mathfrak{a}, \mathfrak{b}$ relativ prime Ideale sind.

Ist unter der Voraussetzung relativ primer Ideale $\mathfrak{a}, \mathfrak{b}$ das Produkt $\mathfrak{b}\mathfrak{c}$ der beiden Ideale $\mathfrak{b}, \mathfrak{c}$ teilbar durch

$\mathfrak{a}$, so muß $\mathfrak{c}$ durch $\mathfrak{a}$ teilbar sein. Denn in diesem Falle besteht wegen $\mathfrak{bc} \succ \mathfrak{a}$ (nach Kap. 2, Nr. 1) die Gleichheit $\mathfrak{a} + \mathfrak{bc} = \mathfrak{a}$, wodurch aus der nach der Voraussetzung gültigen Gleichung (87) die Beziehung

$$\mathfrak{a} + \mathfrak{c} = \mathfrak{a},$$

d. h. (nach derselben Stelle des zweiten Kapitels) die folgende:

$$\mathfrak{c} \succ \mathfrak{a}$$

hervorgeht.

Ist unter der gleichen Voraussetzung ein Ideal $\mathfrak{c}$ durch jedes der Ideale $\mathfrak{a}$, $\mathfrak{b}$ teilbar, so ist es dies auch durch ihr Produkt $\mathfrak{ab}$. Denn aus

$$\mathfrak{c} \succ \mathfrak{a}, \; \mathfrak{c} \succ \mathfrak{b}$$

folgen zwei Gleichungen

$$\mathfrak{c} = \mathfrak{am}, \quad \mathfrak{c} = \mathfrak{bn},$$

wo $\mathfrak{m}$, $\mathfrak{n}$ Ideale bedeuten. Da hiernach das Produkt $\mathfrak{bn}$ teilbar ist durch $\mathfrak{a}$, muß nach dem letzten Satze $\mathfrak{n}$ teilbar durch $\mathfrak{a}$, mithin $\mathfrak{n} = \mathfrak{a} \cdot \mathfrak{q}$ sein, wo $\mathfrak{q}$ ein Ideal. Hieraus folgt

$$\mathfrak{c} = \mathfrak{ab} \, . \, \mathfrak{q},$$

w. z. b. w. (Vgl. Kap. 2, Nr. 4, Ende).

Sind immer noch $\mathfrak{a}$, $\mathfrak{b}$ relativ prime Ideale, so wird auch jeder Idealteiler $\mathfrak{a}'$ von $\mathfrak{a}$ relativ prim sein zu jedem Idealteiler $\mathfrak{b}'$ von $\mathfrak{b}$. Denn für solche Teiler bestehen die Beziehungen

$$\mathfrak{a} \succ \mathfrak{a}', \quad \mathfrak{b} \succ \mathfrak{b}',$$

woraus auch

$$\mathfrak{a} + \mathfrak{b} \succ \mathfrak{a}' + \mathfrak{b}',$$

d. h. nach der Voraussetzung $\mathfrak{g} \succ \mathfrak{a}' + \mathfrak{b}'$ folgt, und da auch umgekehrt $\mathfrak{a}' + \mathfrak{b}' \succ \mathfrak{g}$ sein muß, geht die Gleichung $\mathfrak{a}' + \mathfrak{b}' = \mathfrak{g}$ hervor, welche die Behauptung als richtig erweist.

12. Es ist schon bemerkt worden, daß das Ideal $\mathfrak{g}$ Teiler jedes andern Ideals und so auch, da jedes Ideal als ein Teiler von sich selbst angesehen werden kann, ein Teiler von $\mathfrak{g}$ ist. Das Ideal $\mathfrak{g}$ hat aber keinen Teiler außer sich selbst, denn wäre $\mathfrak{g} \succ \mathfrak{j}$, so folgte in Verbindung mit $\mathfrak{j} \succ \mathfrak{g}$ die Gleichheit $\mathfrak{j} = \mathfrak{g}$. Aus dieser Rücksicht wie wegen der allgemeinen Beziehung $\mathfrak{gj} = \mathfrak{j}$ spielt das Ideal $\mathfrak{g}$ bezüglich der Teilbarkeit der Ideale völlig die Rolle, welche in der gewöhnlichen

Zahlentheorie der Einheit zukommt. Jedes von $\mathfrak{g}$ verschiedene Ideal $\mathfrak{j}$ hat dagegen mindestens zwei Teiler, nämlich $\mathfrak{j}$ und $\mathfrak{g}$. Hat nun ein Ideal keine andern als diese zwei selbstverständlichen Teiler, so wird es *ein Primideal* genannt.

Ist $\mathfrak{p}$ ein Primideal, so ist irgend ein anderes Ideal $\mathfrak{j}$ entweder teilbar durch $\mathfrak{p}$ oder relativ prim zu $\mathfrak{p}$. Denn, da $\mathfrak{p}$ nur die beiden Teiler $\mathfrak{p}$ und $\mathfrak{g}$ besitzt, muß der größte gemeinsame Teiler von $\mathfrak{p}$ und $\mathfrak{j}$ entweder $\mathfrak{p}$, also $\mathfrak{j}$ durch $\mathfrak{p}$ teilbar sein, oder er ist $\mathfrak{g}$, d. h. es besteht die Gleichung

$$\mathfrak{p} + \mathfrak{j} = \mathfrak{g},$$

welche die zweite Alternative zum Ausdrucke bringt.

Ist daher ein Produkt zweier Ideale $\mathfrak{a}, \mathfrak{b}$ teilbar durch ein Primideal $\mathfrak{p}$, so muß auch einer der Faktoren es sein. Denn, wären beide Ideale $\mathfrak{a}, \mathfrak{b}$ relativ prim zu $\mathfrak{p}$, so wäre dem viertletzten Satze der vorigen Nummer zufolge das Produkt $\mathfrak{a}\mathfrak{b}$ gegen die Voraussetzung relativ prim zu $\mathfrak{p}$; da somit eins der Ideale $\mathfrak{a}, \mathfrak{b}$ nicht relativ prim zu $\mathfrak{p}$ sein darf, muß es durch $\mathfrak{p}$ teilbar sein. Oder auch so: Ist $\mathfrak{a}$ nicht teilbar durch $\mathfrak{p}$, so ist es relativ prim zu $\mathfrak{p}$, d. h. es besteht die Gleichung $\mathfrak{g} = \mathfrak{a} + \mathfrak{p}$, aus welcher durch Multiplikation mit $\mathfrak{b}$ die folgende:

$$\mathfrak{b} = \mathfrak{a}\mathfrak{b} + \mathfrak{b}\mathfrak{p}$$

hervorgeht; dieser zufolge und da nach Voraussetzung $\mathfrak{a}\mathfrak{b}$ in $\mathfrak{p}$ enthalten ist, ergibt sich aber die Beziehung

$$\mathfrak{b} \succ \mathfrak{p},$$

mithin ist dann, der Behauptung entsprechend, $\mathfrak{b}$ teilbar durch $\mathfrak{p}$.

Jedes von $\mathfrak{g}$ verschiedene Ideal $\mathfrak{j}$ besitzt einen Primidealteiler. Dies leuchtet ein, wenn $\mathfrak{j}$ selbst ein Primideal ist. Im entgegengesetzten Falle hat $\mathfrak{j}$ außer den Teilern $\mathfrak{g}$ und $\mathfrak{j}$ noch mindestens einen andern Idealteiler $\mathfrak{a}$, sodaß $\mathfrak{j} = \mathfrak{a}\mathfrak{j}'$ gesetzt werden kann. Ist $\mathfrak{j}'$ noch kein Primideal, so besitzt es wieder einen von $\mathfrak{g}$ und $\mathfrak{j}'$ verschiedenen Idealteiler $\mathfrak{a}'$, sodaß $\mathfrak{j}' = \mathfrak{a}'\mathfrak{j}''$ und folglich $\mathfrak{j} = \mathfrak{a}\mathfrak{a}' \cdot \mathfrak{j}''$ gesetzt werden kann usw. Durch Fortsetzung dieser Betrachtung muß man aber endlich

zu einem Primidealteiler von $\mathfrak{j}$ geführt werden, denn sonst könnte man setzen

$$\mathfrak{j} = \mathfrak{a}\mathfrak{a}'\mathfrak{a}'' \cdots \mathfrak{a}^{(i-1)} \cdot \mathfrak{j}^{(i)},$$

während i beliebig groß, z. B. um Eins größer ist, als die nach Nr. 2 endliche Anzahl verschiedener Teiler von $\mathfrak{j}$, welche t heiße; dann würden aber mehr als t voneinander verschiedene Teiler von $\mathfrak{j}$ vorhanden sein, da die $t + 1$ Ideale

$$\mathfrak{a},\ \mathfrak{a}\mathfrak{a}',\ \mathfrak{a}\mathfrak{a}'\mathfrak{a}'', \cdots, \mathfrak{a}\mathfrak{a}' \cdots \mathfrak{a}^{(t-1)},\ \mathfrak{a}\mathfrak{a}' \cdots \mathfrak{a}^{(t-1)}\mathfrak{a}^{(t)}$$

nicht allein offenbar Teiler von $\mathfrak{j}$, sondern auch unter einander verschieden sind, indem aus der Gleichheit zweier von ihnen:

$$\mathfrak{a}\mathfrak{a}' \cdots \mathfrak{a}^{(h-1)} = \mathfrak{a}\mathfrak{a}' \cdots \mathfrak{a}^{(h-1)} \cdot \mathfrak{a}^{(h)} \cdots \mathfrak{a}^{(h+k-1)}$$

die Gleichung

$$\mathfrak{g} = \mathfrak{a}^{(h)} \cdots \mathfrak{a}^{(h+k-1)}$$

hervorginge, welche unmöglich ist, da die Ideale $\mathfrak{a}^{(h)}, \cdots, \mathfrak{a}^{(h+k-1)}$ von $\mathfrak{g}$ verschieden vorausgesetzt worden sind. Somit muß endlich eins der Ideale der Reihe $\mathfrak{j}', \mathfrak{j}'', \mathfrak{j}''', \cdots$ ein Primideal $\mathfrak{p}$ sein, also $\mathfrak{j}$ den Primidealteiler $\mathfrak{p}$ besitzen.

Hieraus folgt aber die Zerlegung des Ideals $\mathfrak{j}$ in eine endliche Anzahl von Primidealfaktoren. Denn zunächst darf man setzen $\mathfrak{j} = \mathfrak{p} \cdot \mathfrak{j}_1$. Ist nun $\mathfrak{j}_1$ schon ein Primideal $\mathfrak{p}_1$, so wäre bereits $\mathfrak{j} = \mathfrak{p}\mathfrak{p}_1$ die gedachte Zerlegung. Andernfalls enthält $\mathfrak{j}_1$ einen Primidealfaktor $\mathfrak{p}_1$, sodaß $\mathfrak{j}_1 = \mathfrak{p}_1\mathfrak{j}_2$, mithin $\mathfrak{j} = \mathfrak{p}\mathfrak{p}_1 \cdot \mathfrak{j}_2$ gesetzt werden kann. Fährt man so fort, so muß in der Reihe der so sich einstellenden Ideale $\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \cdots$ endlich ein letztes ein Primideal sein, wie durch eine der vorigen völlig entsprechende Schlußweise einzusehen ist. Man erhält daher schließlich eine Gleichung von der Form

$$\mathfrak{j} = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r, \tag{88}$$

in welcher sämtliche Faktoren Primideale sind, die jedoch nicht voneinander verschieden zu sein brauchen. Geht hieraus der Satz hervor, daß jedes Ideal in eine endliche Anzahl von Primidealfaktoren zerlegbar ist, so erkennt man leicht weiter, daß solche Zerlegung auch nur auf eine Weise möglich ist. Denn, gäbe es eine zweite:

$$\mathfrak{j} = \mathfrak{q}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s, \tag{89}$$

wo wieder sämtliche Faktoren Primideale bedeuten, so folgte die Gleichung

$$(90)\qquad \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s,$$

der zufolge das Produkt zur Linken durch das Primideal $\mathfrak{q}$ teilbar wäre; $\mathfrak{q}$ müßte mithin Teiler eines der Primideale $\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_r$, und da $\mathfrak{q}$ von $\mathfrak{g}$ verschieden ist, einem dieser Ideale gleich sein. Wäre also etwa $\mathfrak{q} = \mathfrak{p}$, so folgte aus (90) — vgl. den auf (68) bezüglichen Satz — die einfachere Gleichung

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s,$$

aus der durch die gleiche Schlußweise wieder ein Faktor der linken gegen die rechte Seite sich heben würde usw. Man erkennt auf solche Weise, ganz wie in früheren analogen Fällen, die völlige Identität der Zerlegungen (88) und (89) und darf daher, indem man noch die unter einander gleichen Primidealfaktoren immer zu einer Potenz vereinigt, den folgenden Hauptsatz von der Teilbarkeit der Ideale aussprechen:

Ein jedes Ideal $\mathfrak{j}$ kann stets und nur auf eine einzige, völlig bestimmte Weise als ein Produkt aus Potenzen von Primidealen dargestellt werden in der Form

$$(91)\qquad \mathfrak{j} = \mathfrak{p}^{a}\cdot\mathfrak{p}_1^{a_1}\cdot\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r},$$

wo $a, a_1, a_2, \cdots, a_r$ positive ganze Exponenten bedeuten.

13. Dieser allgemeine Satz gilt selbstverständlich auch für den besonderen Fall, wo das Ideal $\mathfrak{j}$ ein Hauptideal, also, unter γ eine ganze Zahl des Körpers verstanden, $\mathfrak{j} = \mathfrak{g}\gamma$ ist. Da nun, wenn das Ideal $\mathfrak{g}\gamma$ durch jedes der Ideale $\mathfrak{p}^{a}, \mathfrak{p}_1^{a_1}, \cdots, \mathfrak{p}_r^{a_r}$ teilbar, d. h. in jedem dieser Ideale enthalten ist, das Gleiche auch von der Zahl γ gilt, und umgekehrt, so darf man die Formel (91) von dem Ideale $\mathfrak{g}\gamma$ auf die Zahl γ übertragen und sie dahin aussprechen: daß auch die ganze *Zahl* γ des Körpers auf eindeutige Weise als Produkt aus einer endlichen Anzahl Potenzen von Primidealen darstellbar sei. Dies Resultat ist aber im allgemeinen durchaus von der Darstellung

$$\gamma = \beta\beta'\beta''\cdots\beta^{(r)}$$

der Zahl γ als Produkt aus einer endlichen Anzahl unzer-

legbarer Zahlen des Körpers, deren Möglichkeit in Kap. 4, Nr. 3 nachgewiesen worden ist, zu unterscheiden. Letztere Zerlegung, welcher, wie dort bemerkt, die Eigenschaft im allgemeinen abgeht, die einzig mögliche zu sein, wodurch die Faktoren sich erst als die eigentlichen Elemente der Zerlegung bezeugen, kann eben deshalb der gedachten Zerlegung der Zahl γ in Primidealfaktoren dann nicht gleichbedeutend sein. Nur in dem Falle, wo diese Primideale lauter Hauptideale, also etwa

$$\mathfrak{p} = \mathfrak{g}\pi, \ \mathfrak{p}_1 = \mathfrak{g}\pi_1, \ \cdots, \ \mathfrak{p}_r = \mathfrak{g}\pi_r$$

sind, unter $\pi, \pi_1, \cdots, \pi_r$ ganze Zahlen des Körpers verstanden, wird die Zerlegung der Zahl γ in das Produkt

$$\mathfrak{p}^a \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

von Idealen bis auf einen Einheitsfaktor mit der entsprechenden Zerlegung der Zahl γ in unzerlegbare Zahlen:

$$\gamma = \pi^a \pi_1^{a_1} \cdots \pi_r^{a_r}$$

in der Tat identisch sein, denn aus $\mathfrak{g}\gamma = \mathfrak{g}\delta$ folgt, daß jede der Zahlen γ, δ ein Vielfaches der anderen, beide also einander assoziiert sein müssen.

Wenn dagegen eins der Ideale, etwa das Ideal $\mathfrak{p}$ kein Hauptideal ist, so ist doch, wie Formel (67) lehrt, $\mathfrak{p}^h$ ein solches, etwa

$$\mathfrak{p}^h = \mathfrak{g}\pi. \tag{92}$$

Setzt man nun $\sqrt[h]{\pi} = \beta$ und nennt φ irgend eine Zahl des Ideals $\mathfrak{p}$, so ist β eine ganze algebraische Zahl, die freilich nicht dem Körper $K(\mathsf{A}; R)$ anzugehören braucht, und φ^h eine Zahl des Ideals $\mathfrak{p}^h$, wegen (92) also teilbar durch $\pi = \beta^h$, mithin φ teilbar durch β; umgekehrt, wenn φ eine ganze Zahl des Körpers, welche durch β teilbar ist, so ist φ^h eine durch $\beta^h = \pi$ teilbare, d. h. im Ideale $\mathfrak{g}\pi = \mathfrak{p}^h$ enthaltene Zahl, oder $\mathfrak{g}\varphi^h = (\mathfrak{g}\varphi)^h$ ist ein durch das Ideal $\mathfrak{p}^h$ und demnach $\mathfrak{g}\varphi$ ein durch $\mathfrak{p}$ teilbares Ideal, d. h. φ eine Zahl in $\mathfrak{p}$. Hiernach darf das Ideal $\mathfrak{p}$ offenbar als die Gesamtheit aller ganzen Zahlen des Körpers aufgefaßt werden, welche durch die Zahl β teilbar sind. Nennt man diese an sich zwar wirkliche ganze algebraische Zahl β, weil sie im allgemeinen dem Körper

$K(\mathsf{A}; R)$ nicht angehört, eine ideale Zahl dieses Körpers, so läßt sich jedem Primideale $\mathfrak{p}$ eine bestimmte ideale Zahl β zuordnen, mit deren, dem Körper angehörigen Vielfachen seine Zahlen identisch sind, und jeder Potenz des Ideals $\mathfrak{p}$ entspricht die gleiche Potenz dieser idealen Zahl β. Unter solchem Gesichtspunkte ist dann die Zerlegung des Hauptideals $\mathfrak{g}\gamma$ oder der ganzen Zahl γ des Körpers in Primidealpotenzen nach der Formel

$$\mathfrak{g}\gamma = \mathfrak{p}^a \cdot \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

völlig gleichbedeutend mit ihrer Zerlegung

$$\gamma = \beta^a \cdot \beta^{a_1} \cdots \beta_r^{a_r}$$

in Potenzen der den Primidealen $\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_r$ resp. zugeordneten idealen Zahlen $\beta, \beta_1, \cdots, \beta_r$.

Man beachte dabei, daß hier nichts auftritt, was nicht wirklich, vielmehr nur, wie dies bei Kummers idealen Teilern der Fall war, als Fiktion vorhanden ist; die Idealität der Zahlen $\beta, \beta_1, \cdots, \beta_r$ besagt eben nur ihre Nichtzugehörigkeit zu dem gerade der Betrachtung vorliegenden endlichen Körper.

14. Hat man durch die Formel (91) ein Ideal $\mathfrak{j}$ in seine Primidealfaktoren zerlegt, so leitet man daraus, ganz wie in der gewöhnlichen Zahlentheorie für eine ganze Zahl, seine sämtlichen Teiler und deren Anzahl her. Ist nämlich $\mathfrak{d}$ irgend ein Idealteiler von $\mathfrak{j}$, also

$$\mathfrak{j} = \mathfrak{d} \cdot \mathfrak{j}', \tag{93}$$

wo auch $\mathfrak{j}'$ ein Ideal bedeutet, und denkt man sich das Ideal $\mathfrak{d}$ in seine Primidealfaktoren zerlegt, so muß jeder solcher Faktor, da er im Produkte (91) aufgeht, in einem seiner Primidealfaktoren aufgehen, d. h. mit einem von diesen identisch sein. Der Teiler $\mathfrak{d}$ von $\mathfrak{j}$ kann also keine anderen Primidealfaktoren haben, als $\mathfrak{j}$ selber besitzt, daher muß

$$\mathfrak{d} = \mathfrak{p}^d \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r} \tag{94}$$

sein, wo jeder der Exponenten d_i positiv oder falls der Idealteiler $\mathfrak{p}_i$ kein Teiler von $\mathfrak{d}$ wäre, gleich Null ist, und jedenfalls nicht größer sein kann als resp. a_i, da sonst der Primfaktor $\mathfrak{p}_i$ aus der linken Seite der Gleichung (93) gehoben, aber in

ihrer rechten Seite verbleiben würde, was unzulässig ist Da nun unter dieser Beschränkung der Exponenten d_i jedes Ideal (94) auch umgekehrt ein Teiler von $\mathfrak{j}$ ist, weil man schreiben kann

$$\mathfrak{j} = \mathfrak{d} \cdot \mathfrak{p}^{a-d} \mathfrak{p}_1^{a_1-d_1} \cdots \mathfrak{p}_r^{a_r-d_r},$$

worin die einzelnen Potenzen positive Primidealpotenzen sind oder, falls $d_i = a_i$ wäre, durch Eins oder durch das Ideal $\mathfrak{g}$ zu ersetzen wären, so ergibt sich das Resultat: Die Formel (94) gibt sämtliche Teiler des Ideals $\mathfrak{j}$ und nur solche, wenn man darin jeden der Exponenten d_i die Reihe

$$d_i = 0, 1, 2, 3, \cdots, a_i \quad (i = 0, 1, 2, \cdots, r)$$

durchlaufen läßt; die Anzahl der Teiler des Ideals $\mathfrak{j}$ beträgt daher

$$(a+1)(a_1+1)\cdots(a_r+1).$$

Offenbar bildet man auch genau nach denselben Regeln, wie in der gewöhnlichen Zahlentheorie, aus den Zerlegungen mehrerer Ideale in ihre Primidealfaktoren den größten gemeinsamen Teiler sowie das kleinste gemeinsame Vielfache derselben. Beschränken wir uns zum Nachweise auf zwei Ideale $\mathfrak{j}$ und $\mathfrak{j}'$, und denken diese in ihre Primidealpotenzen zerlegt. Ihr größter gemeinsamer Teiler $\mathfrak{d} = \mathfrak{j} + \mathfrak{j}'$ kann als Teiler sowohl von $\mathfrak{j}$ als von $\mathfrak{j}'$ nur solche Primidealfaktoren besitzen, welche beiden Zerlegungen gemeinsam sind und darf jeden derselben höchstens so oft enthalten, als er sowohl in der einen wie in der anderen Zerlegung sich findet; demnach ist $\mathfrak{d}$ jedenfalls ein Teiler des Produktes, welches aus den niedrigsten in den Zerlegungen auftretenden Potenzen der ihnen gemeinsamen Primideale gebildet ist, und da umgekehrt dies Produkt offenbar selbst ein gemeinsamer Teiler von $\mathfrak{j}$ und $\mathfrak{j}'$ ist, also in ihrem größten gemeinsamen Teiler $\mathfrak{d}$ aufgehen muß, so ist es dem letzteren gleich. Man erhält also den größten gemeinsamen Teiler zweier Ideale $\mathfrak{j}$ und $\mathfrak{j}'$ aus deren Zerlegungen als das Produkt aus den niedrigsten in diesen auftretenden Potenzen der ihnen gemeinsamen Primideale.

Da ebenso das kleinste gemeinsame Vielfache $\mathfrak{m} = \mathfrak{j} - \mathfrak{j}'$ der beiden Ideale sowohl durch $\mathfrak{j}$ als durch $\mathfrak{j}'$ teilbar ist, muß es durch jede Primidealpotenz, welche in der Zerlegung des einen oder auch des andern von ihnen vorhanden ist, teilbar sein, also jeden in diesen Zerlegungen auftretenden Primidealfaktor mindestens sooft enthalten, als er darin sich findet; $\mathfrak{m}$ ist daher durch das Produkt, welches aus den höchsten in diesen Zerlegungen auftretenden Potenzen sämtlicher darin vorhandenen Primideale gebildet ist, teilbar. Da letzteres aber andererseits offenbar sowohl durch $\mathfrak{j}$ wie durch $\mathfrak{j}'$ teilbar ist, also als gemeinsames Vielfache von $\mathfrak{j}$ und $\mathfrak{j}'$ durch deren kleinstes gemeinsames Vielfache $\mathfrak{m}$ aufgehen muß, so ergibt es sich gleich $\mathfrak{m}$. *Daher findet sich das kleinste gemeinsame Vielfache zweier Ideale $\mathfrak{j}$ und $\mathfrak{j}'$ aus deren Zerlegungen als das aus den höchsten in diesen auftretenden Potenzen aller darin vorhandenen Primideale gebildete Produkt.*

Hiernach lassen sich nun auch die sämtlichen in Nr. 11 bewiesenen Teilbarkeitssätze und mancherlei andere, welche denen der gewöhnlichen Zahlentheorie völlig konform wären, bestätigen bezw. herleiten; wir beschränken uns aber auf den nochmaligen Nachweis der mit (85) übereinstimmenden Formel:

$$(95) \qquad (\mathfrak{j} + \mathfrak{j}') \cdot (\mathfrak{j} - \mathfrak{j}') = \mathfrak{j} \cdot \mathfrak{j}'.$$

Ist nämlich $\mathfrak{p}$ irgend eins der Primideale, welche in den Zerlegungen von $\mathfrak{j}$ und $\mathfrak{j}'$ enthalten sind, so bezeichne $\mathfrak{p}^g$ die höchste darin auftretende Potenz desselben, die eine der Primidealpotenzen in der Zerlegung von $\mathfrak{j} - \mathfrak{j}'$ ausmachen wird. Ist $\mathfrak{p}$ ein Primideal, welches beiden Zerlegungen von $\mathfrak{j}$ und $\mathfrak{j}'$ gemeinsam ist, und $\mathfrak{p}^k$ die niedrigste der darin auftretenden Potenzen von $\mathfrak{p}$, so tritt $\mathfrak{p}^k$ als Primidealpotenz in der Zerlegung von $\mathfrak{j} + \mathfrak{j}'$ auf; findet sich dagegen $\mathfrak{p}$ nur in einer jener Zerlegungen, in welchem Falle man $\mathfrak{p}^k = \mathfrak{p}^0$, wofür auch Eins oder $\mathfrak{g}$ gesetzt werden darf, als die niedrigste in diesen Zerlegungen auftretende Potenz ansehen kann, so tritt es in derjenigen von $\mathfrak{j} + \mathfrak{j}'$ nicht, oder ebenfalls in der Potenz $\mathfrak{p}^k = \mathfrak{p}^0$ auf. Demnach enthält die linke Seite der Gleichung (95) von jedem in den Zerlegungen von $\mathfrak{j}$ und $\mathfrak{j}'$ auftretenden Prim-

idealfaktor $\mathfrak{p}$ die Potenz $\mathfrak{p}^{g+k} = \mathfrak{p}^g \cdot \mathfrak{p}^k$, welche ersichtlich auch die in dem Produkte $\mathfrak{j} \cdot \mathfrak{j}'$ auftretende Potenz dieses Primideals sein muß, und die Gleichung (95) ist somit bestätigt.

Hieran schließen wir noch folgende Betrachtungen. Bereits ist bemerkt worden, daß ein Ideal $\mathfrak{g}\gamma$ dann und nur dann in einem Ideale $\mathfrak{a}$ enthalten oder durch dasselbe teilbar ist, wenn die ganze Zahl γ des Körpers in $\mathfrak{a}$ enthalten ist, und man darf daher eine solche Zahl γ immer zugleich mit dem Hauptideale $\mathfrak{g}\gamma$ teilbar, resp. nicht teilbar nennen durch ein Ideal $\mathfrak{a}$. Daher werden wir auch sagen: der größte gemeinsame Teiler der ganzen Zahl γ des Körpers und des Ideals $\mathfrak{a}$ sei der größte gemeinsame Teiler $\mathfrak{g}\gamma + \mathfrak{a}$ der beiden Ideale $\mathfrak{g}\gamma$ und $\mathfrak{a}$, und werden γ und $\mathfrak{a}$ relativ prim nennen, wenn die beiden Ideale $\mathfrak{g}\gamma$ und $\mathfrak{a}$ es sind, d. h. wenn dieser größte gemeinsame Teiler

$$\mathfrak{g}\gamma + \mathfrak{a} = \mathfrak{g}$$

ist. Somit wären dann zwei ganze Zahlen α_1, α_2 des Körpers relativ prim zu nennen dann und nur dann, wenn die beiden Hauptideale $\mathfrak{g}\alpha_1$, $\mathfrak{g}\alpha_2$ es sind. Man überzeugt sich leicht, daß diese Definition zweier relativ primen Zahlen α_1, α_2 mit der in Nr. 10 aufgestellten völlig identisch ist. In der Tat, sind $\mathfrak{g}\alpha_1$, $\mathfrak{g}\alpha_2$ relativ prime Ideale, so besteht die Gleichung

$$\mathfrak{g}\alpha_1 + \mathfrak{g}\alpha_2 = \mathfrak{g}, \tag{96}$$

daher muß die in $\mathfrak{g}$ enthaltene Zahl 1 sich darstellen lassen in der Form

$$\alpha_1\gamma_1 + \alpha_2\gamma_2 = 1,$$

wo γ_1, γ_2 ganze Zahlen des Körpers sind, mithin sind α_1, α_2 jener Definition gemäß (vgl. (76)) relativ prim. Besteht aber die Gleichung (96) nicht, ist also der größte gemeinsame Teiler $\mathfrak{d}$ der Ideale $\mathfrak{g}\alpha_1$, $\mathfrak{g}\alpha_2$ von $\mathfrak{g}$ verschieden, so ist das in ihrem kleinsten gemeinsamen Vielfachen $\mathfrak{m}$ enthaltene Ideal

$$\mathfrak{g}\alpha_1\alpha_2 = \mathfrak{g}\alpha_1 \cdot \mathfrak{g}\alpha_2 = \mathfrak{m} \cdot \mathfrak{d}$$

verschieden von $\mathfrak{m}$, d. h. es gibt in $\mathfrak{g}$ eine Zahl γ, welche gleichzeitig durch α_1 und durch α_2 und doch nicht durch $\alpha_1\alpha_2$ teilbar ist; daher können dann α_1, α_2, jener Definition entsprechend, nicht relativ prim sein (vgl. letzten Satz Nr. 10).

Die Zahlen α_1, α_2 sind also relativ prim oder nicht, je nachdem die Hauptideale $\mathfrak{g}\alpha_1$, $\mathfrak{g}\alpha_2$ es sind oder nicht sind, w. z. b. w.

15. Wir gehen nun dazu über, Kongruenzen in bezug auf einen Idealmodulus zu betrachten, indem wir wieder zwei ganze Zahlen α, β des Körpers kongruent nennen (mod. $\mathfrak{m}$), in Zeichen:

$$(97) \qquad \alpha \equiv \beta \pmod{\mathfrak{m}},$$

wenn ihre Differenz im Modulus $\mathfrak{m}$ enthalten ist. Ist $\mathfrak{m}$ ein Ideal, so zeichnen derartige Kongruenzen vor den in bezug auf einen beliebigen Modulus $\mathfrak{m}$ genommenen durch eine wichtige Eigenschaft sich aus: sie dürfen nämlich mit irgend einer ganzen Zahl des Körpers, da jede solche in der Ordnung des Idealmodulus (s. Nr. 7) enthalten ist, und, wenn zwei oder mehrere solcher Kongruenzen für denselben Idealmodulus vorliegen, so dürfen auch diese mit einander multipliziert werden. Denn, wenn für $\mathfrak{m} = \mathfrak{j}$ die Kongruenz (97) besteht, also $\alpha - \beta$ eine Zahl in $\mathfrak{j}$ ist, so ist's der Definition eines Ideals zufolge, unter γ irgend eine Zahl in $\mathfrak{g}$ verstanden, auch die Zahl $\gamma(\alpha - \beta) = \gamma\alpha - \gamma\beta$ und folglich ist

$$(98) \qquad \gamma\alpha \equiv \gamma\beta \pmod{\mathfrak{m}}.$$

Desgleichen, wenn neben der Kongruenz (97) auch die folgende besteht:

$$(99) \qquad \alpha' \equiv \beta' \pmod{\mathfrak{m} = \mathfrak{j}},$$

so gehören $\alpha - \beta$ und $\alpha' - \beta'$, folglich auch die Zahlen $(\alpha - \beta)\alpha'$ und $(\alpha' - \beta')\beta$ und daher auch die Zahl

$$(\alpha - \beta)\alpha' + (\alpha' - \beta')\beta = \alpha\alpha' - \beta\beta'$$

dem Ideale an, d. h. es ist

$$(100) \qquad \alpha\alpha' \equiv \beta\beta' \pmod{\mathfrak{m}}.$$

Umgekehrt darf man aus der Kongruenz (98) für $\mathfrak{m} = \mathfrak{j}$ die Kongruenz (97) erschließen, sooft γ eine zum Ideale relativ prime Zahl in $\mathfrak{g}$ bezeichnet. Denn jener Kongruenz zufolge ist das Ideal

$$\mathfrak{g}(\alpha\gamma - \beta\gamma) = \mathfrak{g}\gamma \cdot \mathfrak{g}(\alpha - \beta)$$

durch das Ideal $\mathfrak{m}$ teilbar; da nun nach Voraussetzung das

Ideal $\mathfrak{g}\gamma$ zum Ideale $\mathfrak{m}$ relativ prim ist, muß der andere Faktor $\mathfrak{g}(\alpha - \beta)$ des Produkts durch $\mathfrak{m}$ teilbar sein, d. h. $\alpha - \beta$ ist in $\mathfrak{m}$ enthalten oder die Kongruenz (97) erfüllt.

Schon in Kap. 4, Nr. 7 ist die Anzahl $(\mathfrak{g}, \mathfrak{j})$ der Klassen, in welche die ganzen Zahlen des Körpers (mod. $\mathfrak{j}$) verteilt werden können, als die Norm des Ideales benannt und durch das Zeichen $\mathfrak{N}(\mathfrak{j})$ ausgedrückt, auch gezeigt worden, daß im besonderen die Norm eines Hauptideals $\mathfrak{g}\gamma$ der Absolutwert von der Zahlennorm $N(\gamma)$ ist. Ferner ergibt sich aus Kap. 2, Formel (25) die Kongruenz

$$(\mathfrak{g}, \mathfrak{j}) \cdot \gamma, \text{ d. i. } \mathfrak{N}(\mathfrak{j}) \cdot \gamma \equiv 0 \pmod{\mathfrak{j}}$$

für jede Zahl γ in $\mathfrak{g}$, woraus speziell für $\gamma = 1$ die Kongruenz

$$\mathfrak{N}(\mathfrak{j}) \equiv 0 \pmod{\mathfrak{j}},$$

d. i. der Satz hervorgeht, daß die Norm jedes Ideales eine Zahl dieses Ideales ist.

Nach diesen einfachsten Bemerkungen über Kongruenzen im allgemeinen beweisen wir nun folgenden fundamentalen Satz:

Sind $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ beliebig viel Ideale eines Körpers, welche zu je zweien relativ prim sind, so sind die gleichzeitigen Kongruenzen

$$(101) \quad \omega \equiv \alpha \pmod{\mathfrak{a}}, \quad \omega \equiv \beta \pmod{\mathfrak{b}}, \quad \omega \equiv \gamma \pmod{\mathfrak{c}}, \cdots$$

in denen $\alpha, \beta, \gamma, \cdots$ Zahlen in $\mathfrak{g}$ bedeuten, stets durch eine ebensolche Zahl ω auflösbar, und alle Auflösungen ω sind die Zahlen einer einzigen Klasse kongruenter Zahlen in bezug auf den Modulus

$$\mathfrak{m} = \mathfrak{a}\mathfrak{b}\mathfrak{c} \cdots$$

Dieser Modulus ist einer wiederholten Anwendung des Satzes (86) zufolge das kleinste gemeinsame Vielfache der Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ d. h. die Gesamtheit der Zahlen, welche all' den letzteren gemeinsam sind. Nun kann man nach Nr. 11

$$(102) \qquad \mathfrak{m} = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 = \cdots$$

setzen, während für die Ideale $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \cdots$ die Gleichung erfüllt ist

$$\mathfrak{a}_1 + \mathfrak{b}_1 + \mathfrak{c}_1 + \cdots = \mathfrak{g}.$$

Infolge dieser Beziehung gibt es Zahlen $\alpha_1, \beta_1, \gamma_1, \cdots$ resp. in $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \cdots$, deren Summe

$$(103) \qquad \alpha_1 + \beta_1 + \gamma_1 + \cdots = 1$$

ist. Wenn nun zuerst ω eine Zahl ist, welche den Kongruenzen (101) genügt, so gehören die Zahlen $(\omega - \alpha)\alpha_1$, $(\omega - \beta)\beta_1$, $(\omega - \gamma)\gamma_1, \cdots$ bezw. den Idealen $\mathfrak{a}\mathfrak{a}_1, \mathfrak{b}\mathfrak{b}_1, \mathfrak{c}\mathfrak{c}_1, \cdots$ d. h. sämtlich dem Ideale $\mathfrak{m}$ an, es folgen also die Kongruenzen

$$\omega\alpha_1 \equiv \alpha\alpha_1, \ \omega\beta_1 \equiv \beta\beta_1, \ \omega\gamma_1 \equiv \gamma\gamma_1 \cdots \pmod{\mathfrak{m}}$$

und durch ihre Addition mit Rücksicht auf (103) die folgende:

$$(104) \qquad \omega \equiv \alpha\alpha_1 + \beta\beta_1 + \gamma\gamma_1 + \cdots \quad \pmod{\mathfrak{m}}.$$

Umgekehrt aber genügt jede Zahl ω, welche der durch letztere Kongruenz bestimmten Klasse (mod. $\mathfrak{m}$) angehört, den sämtlichen Kongruenzen (101). Aus den Gleichheiten (102) folgt nämlich, da das Ideal $\mathfrak{a}$ zu jedem der Ideale $\mathfrak{b}, \mathfrak{c}, \cdots$ prim ist, daß die Ideale $\mathfrak{b}_1, \mathfrak{c}_1, \cdots$ durch $\mathfrak{a}$ teilbar, mithin die Zahlen $\beta_1, \gamma_1, \cdots$ in $\mathfrak{a}$ enthalten sind. Ist also ω durch die Kongruenz (104) bestimmt, so folgt, da jede in $\mathfrak{m}$ enthaltene Zahl auch in $\mathfrak{a}$ vorhanden ist, dieselbe Kongruenz auch (mod. $\mathfrak{a}$) und alsdann daraus die einfachere

$$\omega \equiv \alpha\alpha_1 \quad \pmod{\mathfrak{a}}$$

und, da α_1 wegen (103) kongruent 1 ist (mod. $\mathfrak{a}$), noch einfacher

$$\omega \equiv \alpha \quad \pmod{\mathfrak{a}}.$$

In gleicher Weise aber zeigen sich auch die übrigen der Kongruenzen (104) befriedigt; die Formel (104) lehrt also nicht nur deren Möglichkeit, sondern gibt auch ihre vollständige Auflösung an.

Dieselbe Formel (104) liefert ein vollständiges Restsystem für die Zahlen ω in $\mathfrak{g}$ (mod. $\mathfrak{m}$), wenn $\alpha, \beta, \gamma, \cdots$ resp. vollständige Restsysteme dieser Zahlen in bezug auf die Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ durchlaufen. Denn erstens liefert jede der Restkombinationen $\alpha, \beta, \gamma, \cdots$, wie gezeigt, durch die Formel (104) einen bestimmten Rest ω (mod. $\mathfrak{m}$); zweitens entsprechen zwei verschiedenen Rest-

kombinationen $\alpha, \beta, \gamma, \cdots$ und $\alpha', \beta', \gamma', \cdots$ auch verschiedene Reste (mod. $\mathfrak{m}$), da aus der Kongruenz

$$\alpha\alpha_1 + \beta\beta_1 + \cdots \equiv \alpha'\alpha_1 + \beta'\beta_1 + \cdots \pmod{\mathfrak{m}}$$

in der zuvor angegebenen Weise sich $\alpha' \equiv \alpha \pmod{\mathfrak{a}}$, $\beta' \equiv \beta \pmod{\mathfrak{b}}$, $\cdots$ ergäbe; drittens aber muß so auch jeder der verschiedenen Reste (mod. $\mathfrak{m}$) erhalten werden, da notwendig jeder Zahl ω in $\mathfrak{g}$ eine bestimmte der Restkombinationen $\alpha, \beta, \gamma, \cdots$ zugehört.

Nun haben zwei (mod. $\mathfrak{a}$) kongruente Zahlen α, ω immer den gleichen größten gemeinsamen Teiler mit $\mathfrak{a}$, sodaß

$$\mathfrak{g}\alpha + \mathfrak{a} = \mathfrak{g}\omega + \mathfrak{a} \tag{105}$$

ist. Denn, wenn $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ Zahlen in $\mathfrak{a}$ bezeichnen, so ergeben sich aus der Annahme, nach welcher $\omega = \alpha + \alpha_0$ gesetzt werden kann, für jede Zahl γ in $\mathfrak{g}$ die Gleichungen

$$\gamma\alpha + \alpha_1 = \gamma(\omega - \alpha_0) + \alpha_1 = \gamma\omega + \alpha_2$$
$$\gamma\omega + \alpha_2 = \gamma(\alpha + \alpha_0) + \alpha_2 = \gamma\alpha + \alpha_3,$$

woraus die Beziehungen

$$\mathfrak{g}\alpha + \mathfrak{a} \succ \mathfrak{g}\omega + \mathfrak{a}$$
$$\mathfrak{g}\omega + \mathfrak{a} \succ \mathfrak{g}\alpha + \mathfrak{a}$$

also die Gleichung (105) hervorgeht.

Hiernach werden sämtliche Zahlen einer Klasse (mod. $\mathfrak{a}$) relativ prim zu $\mathfrak{a}$ sein, wenn eine von ihnen es ist.

Dies vorausgeschickt, nehmen wir jetzt an, die in den Kongruenzen (101) gegebenen Zahlen $\alpha, \beta, \gamma, \cdots$ seien bezw. zu den Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$ relativ prim. Dann wird auch ihre durch (104) angegebene Lösung ω relativ prim zu $\mathfrak{m}$, nämlich

$$\mathfrak{g}\omega + \mathfrak{m} = \mathfrak{g}$$

sein. Denn sonst hätte $\mathfrak{g}\omega$ mit $\mathfrak{m}$ einen von $\mathfrak{g}$ verschiedenen größten gemeinsamen Teiler, mithin auch einen Primidealfaktor $\mathfrak{p}$ gemeinsam, der in einem der Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$, etwa in $\mathfrak{a}$ aufgehen müßte, und da $\omega \equiv \alpha \pmod{\mathfrak{a}}$ ist, müßte

$$\mathfrak{g}\omega + \mathfrak{a} = \mathfrak{g}\alpha + \mathfrak{a} \succ \mathfrak{p}$$

sein, während es doch nach Voraussetzung gleich $\mathfrak{g}$ ist. Aber auch umgekehrt müssen $\alpha, \beta, \gamma, \cdots$ zu ihren bezüglichen Moduln relativ prim sein, damit ω prim sei zu $\mathfrak{m}$; denn, sobald auch nur eine jener Zahlen, etwa α mit dem bezüglichen Modulus $\mathfrak{a}$ einen von $\mathfrak{g}$ verschiedenen größten gemeinsamen Teiler $\mathfrak{d}$ hätte, mithin $\mathfrak{g}\omega + \mathfrak{a} = \mathfrak{g}\alpha + \mathfrak{a} = \mathfrak{d}$ wäre, würde

$$\mathfrak{g}\omega + \mathfrak{m} \succ \mathfrak{g}\omega + \mathfrak{a} \text{ d. i. } \succ \mathfrak{d}$$

sein, also nicht gleich $\mathfrak{g}$ sein können, ω wäre also nicht relativ prim zu $\mathfrak{m}$. Wir schließen daher den Satz:

Die Lösung (104) der Kongruenzen (101) ist dann und nur dann relativ prim zu $\mathfrak{m}$, wenn die Zahlen $\alpha, \beta, \gamma, \cdots$ sämtlich relativ prim sind bezw. zu $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \cdots$. Nennt man daher allgemein $\varphi(\mathfrak{m})$ die Anzahl derjenigen Klassen (mod. $\mathfrak{m}$) kongruenter Zahlen in $\mathfrak{g}$, deren Glieder relativ prim sind zu $\mathfrak{m}$, so besteht die Beziehung

$$\varphi(\mathfrak{m}) = \varphi(\mathfrak{a}) \cdot \varphi(\mathfrak{b}) \cdot \varphi(\mathfrak{c}) \cdots, \tag{106}$$

sooft

$$\mathfrak{m} = \mathfrak{a} \cdot \mathfrak{b} \cdot \mathfrak{c} \cdots$$

eine Zerlegung des Ideals $\mathfrak{m}$ in relativ prime Faktoren bedeutet.

16. Aus diesen allgemeinen Resultaten fließt eine ganze Reihe anderer Sätze, die zunächst entwickelt werden sollen. Vor allem wird der folgende Satz behauptet:

Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Ideale, so gibt es eine Zahl ω in $\mathfrak{g}$, für welche

$$\mathfrak{a}\mathfrak{b} + \mathfrak{g}\omega = \mathfrak{a} \tag{107}$$

ist. Um dies zu beweisen, sei, in Primidealpotenzen zerlegt,

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}^{a}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r};$$

da $\mathfrak{a}$ ein Teiler von $\mathfrak{a}\mathfrak{b}$, so hat es die Form

$$\mathfrak{a} = \mathfrak{p}^{d}\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r},$$

worin die Exponenten d_i positive ganze Zahlen $\overline{\leq} a_i$ oder Null sind. Man wähle nun für jeden der Indizes $i = 0, 1, 2, \cdots, r$ eine Zahl α_i, welche in $\mathfrak{p}_i^{d_i}$ aber nicht in $\mathfrak{p}_i^{d_i+1}$ enthalten ist,

was möglich ist, da dieser Modulus nur einen Teil von jenem ausmacht; falls $d_i = 0$, kommt diese Wahl von α_i darauf hinaus, für α_i eine nicht im Ideale $\mathfrak{p}_i$ enthaltene ganze Zahl zu nehmen. Dann ist jede, die Kongruenzen

$$(108) \qquad \omega \equiv \alpha \pmod{\mathfrak{p}^{d+1}}, \quad \omega \equiv \alpha_1 \pmod{\mathfrak{p}_1^{d_1+1}}, \cdots, \quad \omega \equiv \alpha_r \pmod{\mathfrak{p}_r^{d_r+1}}$$

erfüllende Zahl, wie es deren nach dem allgemeinen Satze der vorigen Nummer gibt, da die Moduln der Kongruenzen relativ prim sind, eine Zahl, wie der Satz sie behauptet. In der Tat, wenn die Zahl ω den Kongruenzen (108) genügt, so erfüllt sie auch die Kongruenzen

$$\omega \equiv \alpha \pmod{\mathfrak{p}^{d}}, \quad \omega \equiv \alpha_1 \pmod{\mathfrak{p}_1^{d_1}}, \cdots \omega \equiv \alpha_r \pmod{\mathfrak{p}_r^{d_r}},$$

d. h. ω also auch $\mathfrak{g}\omega$ ist, wie die Zahlen α_i, in den untereinander relativ primen Idealen $\mathfrak{p}_i^{d_i}$ und daher auch (Nr. 11, vorletzter Satz) in ihrem Produkte $\mathfrak{a}$ enthalten oder teilbar durch $\mathfrak{a}$. Das Ideal $\mathfrak{g}\omega$ hat aber keins der Primideale $\mathfrak{p}_i$ von $\mathfrak{a}\mathfrak{b}$ öfter zum Faktor als $\mathfrak{a}$, da keine der Zahlen $\alpha_i \equiv 0$ ist (mod. $\mathfrak{p}_i^{d_i+1}$); demnach muß in der Tat $\mathfrak{a}$ der größte gemeinsame Teiler von $\mathfrak{g}\omega$ und $\mathfrak{a}\mathfrak{b}$ sein, wie behauptet.

Man bemerke, daß, wenn ω eine die Bedingung (107) erfüllende Zahl ist, zugleich

$$(109) \qquad \mathfrak{a}\mathfrak{b} - \mathfrak{g}\omega = \mathfrak{b}\omega$$

sein muß. Denn nach (95) besteht die Beziehung

$$(\mathfrak{a}\mathfrak{b} + \mathfrak{g}\omega) \cdot (\mathfrak{a}\mathfrak{b} - \mathfrak{g}\omega) = \mathfrak{a}\mathfrak{b} \cdot \mathfrak{g}\omega,$$

aus welcher das Gesagte hervorgeht.

Hieraus schließen wir weiter den Satz, daß die Norm eines Produkts zweier Ideale gleich dem Produkte aus den Normen seiner Faktoren ist, in Zeichen:

$$(110) \qquad \mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b}).$$

Wählt man nämlich die Zahl ω der Gleichung (107) entsprechend, sodaß auch (109) besteht, so folgt aus den Formeln (19) und (20) des zweiten Kapitels

$$(111) \qquad \begin{aligned} (\mathfrak{g}\omega, \mathfrak{a}\mathfrak{b}) &= (\mathfrak{g}\omega + \mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{a}, \mathfrak{a}\mathfrak{b}) \\ (\mathfrak{g}\omega, \mathfrak{a}\mathfrak{b}) &= (\mathfrak{g}\omega, \mathfrak{a}\mathfrak{b} - \mathfrak{g}\omega) = (\mathfrak{g}\omega, \mathfrak{b}\omega), \end{aligned}$$

welch' letzterer Ausdruck, wie leicht einleuchtet, mit $(\mathfrak{g}, \mathfrak{b})$ gleich ist, da für Zahlen α, β, welche (mod. $\mathfrak{b}$) kongruent sind, offenbar die Produkte $\alpha\omega$, $\beta\omega$ (mod. $\mathfrak{b}\omega$) kongruent sind, und umgekehrt. Da ferner

$$\mathfrak{a}\mathfrak{b} \succ \mathfrak{a} \succ \mathfrak{g}$$

ist, folgt nach der Formel (21) ebendaselbst

$$(\mathfrak{g}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{g}, \mathfrak{a}) \cdot (\mathfrak{a}, \mathfrak{a}\mathfrak{b}),$$

und da aus (111) sich

$$(111^a) \qquad (\mathfrak{a}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{g}, \mathfrak{b})$$

ergibt, geht die Gleichung

$$(\mathfrak{g}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{g}, \mathfrak{a}) \cdot (\mathfrak{g}, \mathfrak{b})$$

hervor, welche mit (110) übereinstimmt.

Die Formel (110) ermöglicht nun in Verbindung mit (106), den Wert der zahlentheoretischen Funktion $\varphi(\mathfrak{m})$ mittels der Primideale, aus welchen $\mathfrak{m}$ selbst zusammengesetzt ist, anzugeben. Wenn

$$(112) \qquad \mathfrak{m} = \mathfrak{p}^a \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

gedacht wird, so genügt es nach der Formel (106), die Funktion $\varphi(\mathfrak{p}^a)$ zu bestimmen, welche die Anzahl der zu $\mathfrak{p}^a$ primen Klassen (mod. $\mathfrak{p}^a$) kongruenter Zahlen in $\mathfrak{g}$ bezeichnet. Alle Zahlen in $\mathfrak{g}$ sind aber entweder relativ prim zu $\mathfrak{p}^a$ oder teilbar durch $\mathfrak{p}$, d. h. im Ideale $\mathfrak{p}$ enthalten, und da für die Zahlen einer Klasse der größte, also auch jeder mit dem Modulus gemeinsame Teiler immer allen gemeinschaftlich ist, zerfallen die sämtlichen $(\mathfrak{g}, \mathfrak{p}^a)$ Klassen der Zahlen in $\mathfrak{g}$, welche für den Modulus $\mathfrak{p}^a$ vorhanden sind, in die $\varphi(\mathfrak{p}^a)$ Klassen der zu $\mathfrak{p}^a$ relativ primen und in die $(\mathfrak{p}, \mathfrak{p}^a)$ Klassen, in welche die durch $\mathfrak{p}$ teilbaren Zahlen sich (mod. $\mathfrak{p}^a$) verteilen, sodaß die Gleichung besteht

$$(113) \qquad (\mathfrak{g}, \mathfrak{p}^a) = \varphi(\mathfrak{p}^a) + (\mathfrak{p}, \mathfrak{p}^a).$$

Da aber $\mathfrak{p}^a \succ \mathfrak{p} \succ \mathfrak{g}$ ist, so gilt nach Kap. 2, Formel (21) die Beziehung

$$(\mathfrak{g}, \mathfrak{p}^a) = (\mathfrak{g}, \mathfrak{p}) \cdot (\mathfrak{p}, \mathfrak{p}^a),$$

der auch die Form

$$\mathfrak{N}(\mathfrak{p}^a) = \mathfrak{N}(\mathfrak{p}) \cdot (\mathfrak{p}, \mathfrak{p}^a)$$

gegeben werden kann und aus welcher, da nach (110)

$$\mathfrak{N}(\mathfrak{p}^a) = \mathfrak{N}(\mathfrak{p})^a$$

ist, sich

$$(\mathfrak{p}, \mathfrak{p}^a) = \mathfrak{N}(\mathfrak{p})^{a-1}$$

ergibt. Infolge dieser Gleichung liefert (113) die Bestimmung

$$\varphi(\mathfrak{p}^a) = \mathfrak{N}(\mathfrak{p})^a - \mathfrak{N}(\mathfrak{p})^{a-1}, \tag{114}$$

eine Gleichung, der man die ähnlichen

$$\varphi(\mathfrak{p}^{a-1}) = \mathfrak{N}(\mathfrak{p})^{a-1} - \mathfrak{N}(\mathfrak{p})^{a-2}$$
$$\cdots\cdots\cdots$$
$$\varphi(\mathfrak{p}^2) = \mathfrak{N}(\mathfrak{p})^2 - \mathfrak{N}(\mathfrak{p})$$
$$\varphi(\mathfrak{p}) = \mathfrak{N}(\mathfrak{p}) - 1$$

an die Seite stellen darf, insbesondere die letzte, da in der Tat die sämtlichen Zahlen in $\mathfrak{g}$ (mod. $\mathfrak{p}$) in die zu $\mathfrak{p}$ relativ primen und die in $\mathfrak{p}$ enthaltenen, welche nur eine Klasse (mod. $\mathfrak{p}$) liefern, zerfallen. Hieraus entnimmt man zunächst die Gleichung

$$1 + \varphi(\mathfrak{p}) + \varphi(\mathfrak{p}^2) + \cdots + \varphi(\mathfrak{p}^a) = \mathfrak{N}(\mathfrak{p}^a).$$

Ebenso findet sich für die andern Primideale der Formel (112)

$$1 + \varphi(\mathfrak{p}_1) + \varphi(\mathfrak{p}_1^2) + \cdots + \varphi(\mathfrak{p}_1^{a_1}) = \mathfrak{N}(\mathfrak{p}_1^{a_1})$$
$$\cdots\cdots\cdots$$
$$1 + \varphi(\mathfrak{p}_r) + \varphi(\mathfrak{p}_r^2) + \cdots + \varphi(\mathfrak{p}_r^{a_r}) = \mathfrak{N}(\mathfrak{p}_r^{a_r}).$$

Die Multiplikation dieser $r+1$ Gleichungen mit einander ergibt links als allgemeines Glied den Ausdruck

$$\varphi(\mathfrak{p}^d)\ \varphi(\mathfrak{p}_1^{d_1}) \cdots \varphi(\mathfrak{p}_r^{d_r}),$$

wo die Exponenten d_i wie in der Formel (94) bestimmt sind, d. h. der Gleichung (106) zufolge den Ausdruck $\varphi(\mathfrak{d})$, unter $\mathfrak{d}$ jeden Teiler von $\mathfrak{m}$ verstanden; die ganze linke Seite der entstehenden Gleichung ist also die auf alle diese Teiler $\mathfrak{d}$ von $\mathfrak{m}$ erstreckte Summe $\sum \varphi(\mathfrak{d})$, während die rechte Seite nach (110) gleich $\mathfrak{N}(\mathfrak{m})$ ist. Man findet daher die Beziehung

$$\sum \varphi(\mathfrak{d}) = \mathfrak{N}(\mathfrak{m}), \tag{115}$$

welche einer bekannten, auf die *Euler*sche Funktion $\varphi(m)$ bezüglichen Formel der gewöhnlichen Zahlentheorie vollkommen analog ist.

Ferner aber ergibt sich aus (114) für

$$\varphi(\mathfrak{m}) = \varphi(\mathfrak{p}^a) \cdot \varphi(\mathfrak{p}_1^{a_1}) \cdots \varphi(\mathfrak{p}_r^{a_r})$$

der folgende Ausdruck

$$(116)\quad \varphi(\mathfrak{m}) = \mathfrak{N}(\mathfrak{m}) \cdot \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)\left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_1)}\right) \cdots \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}_r)}\right),$$

eine Formel, welche ebenfalls das getreue Analogon für die Formel ist, durch welche die Anzahl der zu einer ganzen rationalen Zahl m relativ primen Reste oder Klassen kongruenter Zahlen (mod. m) aus den Primfaktoren von m bestimmt wird.

17. Mit dem ersten Satze voriger Nummer ist ein anderer völlig gleichbedeutend, den wir folgendermaßen aussprechen: Sind $\mathfrak{a}$, $\mathfrak{b}$ beliebige Ideale eines Körpers, so läßt sich $\mathfrak{a}$ stets durch Multiplikation mit einem zu $\mathfrak{b}$ relativ primen Ideale $\mathfrak{m}$ in ein Hauptideal verwandeln. In der Tat, bestimmt man eine Zahl ω, wie sie jener Satz angibt, so ist der Gleichung (107) gemäß $\mathfrak{g}\omega \succ \mathfrak{a}$, so daß man setzen kann

$$\mathfrak{g}\omega = \mathfrak{a} \cdot \mathfrak{m},$$

worauf jene Gleichung die Form annimmt

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{m}) = \mathfrak{a},$$

also

$$\mathfrak{b} + \mathfrak{m} = \mathfrak{g},$$

d. h. $\mathfrak{b}$ und $\mathfrak{m}$ als relativ prime Ideale ergibt; der neue Satz folgt also aus dem früheren. Aber auch umgekehrt; denn, gibt es ein zu $\mathfrak{b}$ relativ primes Ideal $\mathfrak{m}$ von der Beschaffenheit, daß $\mathfrak{a}\mathfrak{m}$ ein Hauptideal $\mathfrak{g}\omega$ wird, so wird, da $\mathfrak{b} + \mathfrak{m} = \mathfrak{g}$ ist,

$$\mathfrak{a}\mathfrak{b} + \mathfrak{g}\omega = \mathfrak{a}\,\mathfrak{b} + \mathfrak{a}\mathfrak{m} = \mathfrak{a}(\mathfrak{b} + \mathfrak{m}) = \mathfrak{a},$$

ω also eine Zahl, wie der frühere Satz sie behauptet.

Weiter erkennt man nunmehr, daß jedes Ideal $\mathfrak{a}$ als größter gemeinsamer Teiler zweier Hauptideale dargestellt werden kann. Ist nämlich α irgend eine in $\mathfrak{a}$ enthaltene (von Null verschiedene) Zahl, so ist auch $\mathfrak{g}\alpha \succ \mathfrak{a}$, es besteht folglich eine Gleichung $\mathfrak{g}\alpha = \mathfrak{a}\mathfrak{b}$, in welcher auch $\mathfrak{b}$ ein Ideal ist; wird nun die Zahl ω den vorigen Sätzen gemäß gewählt, so ergibt sich

$$\mathfrak{a}\mathfrak{b} + \mathfrak{g}\omega, \quad \text{d. i.} \quad \mathfrak{g}\alpha + \mathfrak{g}\omega = \mathfrak{a},$$

wie behauptet. In der Bezeichnungsweise des 3. Kapitels drückt dieser Satz sich dahin aus, daß jedes Ideal in der Form

$$\{\alpha, \omega\}$$

dargestellt werden kann, worin α, ω ganze Zahlen des Körpers sind.

Bei der Bedeutung dieses Satzes mag es erwünscht sein, noch eine zweite Herleitung desselben, wie Hurwitz[1]) sie gegeben hat, kennen zu lernen. Sie beruht auf folgendem Hilfssatze:

Sind α, β, γ drei ganze Zahlen des Körpers, unter denen α nicht Null ist, so gibt es eine ganze Zahl λ des Körpers von der Beschaffenheit, daß

$$(117) \qquad \{\alpha, \beta, \gamma\} = \{\alpha, \beta + \lambda\gamma\}$$

ist. Man darf zum Beweise auch β, γ von Null verschieden voraussetzen, da für $\gamma = 0$ die Formel selbstverständlich ist, für $\beta = 0$ aber durch $\lambda = 1$ erfüllt wird. Bei solcher Voraussetzung darf man dann setzen

$$(118) \qquad \mathfrak{g}\alpha = \mathfrak{d}\mathfrak{a}, \quad \mathfrak{g}\beta = \mathfrak{d}\mathfrak{b}, \quad \mathfrak{g}\gamma = \mathfrak{d}\mathfrak{c},$$

unter $\mathfrak{d}$ das Ideal $\{\alpha, \beta, \gamma\}$ verstehend, welches den größten gemeinsamen Teiler der genannten drei Hauptideale ausmacht, während $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ drei Ideale bezeichnen, für welche

$$(119) \qquad \mathfrak{a} + \mathfrak{b} + \mathfrak{c} = \mathfrak{g}$$

ist. Wenn nun etwa $\mathfrak{a} = \mathfrak{g}$ ist, so wird nach der ersten der Formeln (118)

$$\mathfrak{d} = \{\alpha, \beta, \gamma\} = \{\alpha\},$$

wofür, da der zweiten jener Formeln zufolge β in $\mathfrak{d}$ enthalten, d. h. ein Vielfaches von α ist, auch

$$\{\alpha, \beta, \gamma\} = \{\alpha, \beta\}$$

geschrieben werden kann; demnach findet in diesem Falle für $\lambda = 0$ der Satz statt. Ist dagegen $\mathfrak{a}$ von $\mathfrak{g}$ verschieden, so sei, in Primidealpotenzen zerlegt,

$$\mathfrak{a} = \mathfrak{p}_0^{a_0}\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}$$

1) Hurwitz, zur Theorie der algebraischen Zahlen, Götting. Nachr. 1895.

und $\mathfrak{p}_i^{d_i}$ die höchste Potenz von $\mathfrak{p}_i$, welche in $\mathfrak{d}$ aufgeht, sodaß $d_i = 0$, wenn etwa $\mathfrak{d}$ den Primidealfaktor $\mathfrak{p}_i$ nicht besitzt; endlich bezeichne λ_i die Null oder die Eins, jenachdem das Ideal $\mathfrak{g}\beta$, welches wegen (118) durch $\mathfrak{p}_i^{d_i}$ aufgeht, durch $\mathfrak{p}_i^{d_i+1}$ nicht teilbar oder teilbar ist. Es leuchtet ein, daß, wenn $\lambda_i = 1$, das Ideal $\mathfrak{g}\gamma$, welches ebenfalls durch $\mathfrak{p}_i^{d_i}$ teilbar ist, nicht durch $\mathfrak{p}_i^{d_i+1}$ aufgehen kann, da dann selbst für $d_i = 0$ die Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ entgegen der Gleichung (119) den Teiler $\mathfrak{p}_i$ gemeinsam hätten. Demnach findet für jeden Index $i = 0, 1, 2, \cdots, r$ die Kongruenz

$$\beta + \lambda_i \gamma \equiv 0$$

zwar (mod. $\mathfrak{p}_i^{d_i}$), aber nicht (mod. $\mathfrak{p}_i^{d_i+1}$) statt. Bestimmt man also eine Zahl λ, welche die Kongruenzen

$$\lambda \equiv \lambda_0 \,(\text{mod.}\,\mathfrak{p}_0^{d_0+1}),\ \lambda \equiv \lambda_1 \,(\text{mod.}\,\mathfrak{p}_1^{d_1+1}), \cdots, \lambda \equiv \lambda_r \,(\text{mod.}\,\mathfrak{p}_r^{d_r+1})$$

erfüllt, so wird die ganze Zahl

$$\beta + \lambda\gamma$$

durch jede der in $\mathfrak{d}$ aufgehenden Primidealpotenzen $\mathfrak{p}_i^{d_i}$ aber durch keine höheren teilbar sein, sodaß, wenn

$$\mathfrak{g}(\beta + \lambda\gamma) = \mathfrak{d} \cdot \mathfrak{n}$$

gesetzt wird, das Ideal $\mathfrak{n}$ keinen Primteiler von $\mathfrak{a}$ mehr besitzt, also $\mathfrak{a} + \mathfrak{n} = \mathfrak{g}$ ist. In Beachtung der Gleichungen (118) und (119) findet sich demnach

$$\mathfrak{d} = \mathfrak{g}\alpha + \mathfrak{g}\beta + \mathfrak{g}\gamma = \mathfrak{g}\alpha + \mathfrak{g}(\beta + \lambda\gamma),$$

d. h. die Formel (117) bestätigt.

Nunmehr aber leuchtet ein, daß eine wiederholte Anwendung dieses Hilfssatzes jedes Ideal

$$\{\alpha, \beta, \gamma, \cdots, \zeta\}$$

auf die Form eines zweiteiligen Ideals $\{\alpha, \omega\}$ zurückführt, w. z. b. w.

Hieran schließt sich die Frage, wann zwei Ideale $\{\alpha, \omega\}$ und $\{\alpha', \omega'\}$ einander gleich sind. Sie wird beantwortet durch den ebenfalls von Hurwitz[1]) gegebenen Satz: Damit zwei Ideale $\{\alpha, \omega\}$, $\{\alpha', \omega'\}$ einander gleich sind, ist not-

1) Hurwitz, die unimodularen Substitutionen in einem algebraischen Zahlenkörper, Götting. Nachr. 1895.

wendig und hinreichend, daß die Zahlenpaare α, ω; α', ω' einander äquivalent sind, d. h. daß

$$(120) \qquad \alpha' = \lambda\alpha + \mu\omega, \quad \omega' = \nu\alpha + \varrho\omega$$

ist, während $\lambda, \mu, \nu, \varrho$ ganze Zahlen des Körpers bedeuten, welche der Bedingung

$$(121) \qquad \lambda\varrho - \mu\nu = 1$$

genügen. Bestehen nämlich die Gleichungen (120) und (121), so folgt

$$\alpha = \varrho\alpha' - \mu\omega', \quad \omega = -\nu\alpha' + \lambda\omega'$$

und jede Zahl des Ideals $\{\alpha', \omega'\}$ gehört demnach dem Ideale $\{\alpha, \omega\}$ an, und umgekehrt. Sind andererseits beide Ideale einander gleich, in Zeichen:

$$\mathfrak{j} = \{\alpha, \omega\} = \{\alpha', \omega'\},$$

und setzt man, wie in Nr. 10

$$\mathfrak{j}^h = \mathfrak{g}\gamma, \quad \gamma_0 = \sqrt[h]{\gamma},$$

so bestehen (vgl. Formel (74)) zwei Gleichungen von der Form

$$\gamma_0^h = \alpha\xi + \omega\eta, \quad \gamma_0^h = \alpha'\xi' + \omega'\eta',$$

in denen α, ω und α', ω' durch γ_0, dagegen ξ, η, ξ', η' durch γ_0^{h-1} teilbare ganze Zahlen des Körpers sind. Daher werden die Zahlen

$$\lambda = \frac{\alpha'\xi + \omega\eta'}{\gamma}, \quad \mu = \frac{\alpha'\eta - \alpha\eta'}{\gamma}$$

$$\nu = \frac{\omega'\xi - \omega\xi'}{\gamma}, \quad \varrho = \frac{\omega'\eta + \alpha\xi'}{\gamma},$$

für welche, wie einfach zu übersehen, die Gleichungen (120) und (121) erfüllt sind, ganze Zahlen des Körpers und demnach die Zahlen α', ω' äquivalent sein mit α, ω.

Die Zahl $\zeta = \frac{\alpha}{\omega}$ soll die dem Ideale $\{\alpha, \omega\}$ zugehörige Zahl des Körpers heißen. Da jede Zahl ζ des Körpers und zwar auf mannigfache Weise als der Quotient von zwei ganzen algebraischen Zahlen desselben gedacht werden kann, indem z. B. nach Nr. 2 des 4. Kapitels jede solche Zahl, mit einer gewissen ganzen rationalen Zahl multipliziert, zu einer ganzen algebraischen Zahl des Körpers wird, so ist auch jede solche Zahl ζ einem Ideale zugeordnet. Hier gilt

aber der Satz: Jede Zahl des Körpers ist stets einer ganzen *Klasse* äquivalenter Ideale zugeordnet, und umgekehrt sind alle ein- und derselben Klasse zugeordneten Zahlen unter einander äquivalent. In der Tat, ist $\zeta = \frac{\alpha'}{\omega'}$ eine Zahl des Körpers, so ist sie dem Ideale $\{\alpha', \omega'\}$ zugeordnet; wenn nun $\{\alpha, \omega\}$ ein beliebiges, dem letzteren äquivalentes Ideal bezeichnet, so gibt es zwei ganze Zahlen ψ, ψ' des Körpers von der Beschaffenheit, daß

$$(122) \qquad \psi \cdot \{\alpha', \omega'\} = \psi' \cdot \{\alpha, \omega\}$$

ist, d. h. nach dem vorigen Satze, daß zwei Gleichungen bestehen von der Form

$$(123) \quad \psi \cdot \alpha' = \lambda \cdot \alpha\psi' + \mu \cdot \omega\psi', \quad \psi \cdot \omega' = \nu \cdot \alpha\psi' + \varrho \cdot \omega\psi',$$

während

$$(123^a) \qquad \lambda\varrho - \mu\nu = 1$$

ist. Daraus folgt durch Division

$$\zeta = \frac{\alpha'}{\omega'} = \frac{\lambda\alpha + \mu\omega}{\nu\alpha + \varrho\omega}$$

und somit ist die Zahl ζ auch dem Ideale

$$\{\lambda\alpha + \mu\omega, \ \nu\alpha + \varrho\omega\}$$

zugeordnet, welches dem vorigen Satze zufolge mit $\{\alpha, \omega\}$ identisch ist. Wenn dagegen $\zeta = \frac{\alpha}{\omega}$, $\zeta' = \frac{\alpha'}{\omega'}$ zwei Zahlen des Körpers sind, welche derselben Idealklasse zugeordnet sind, so müssen die Ideale

$$\{\alpha, \omega\}, \quad \{\alpha', \omega'\}$$

einander äquivalent, also eine Gleichung von der Form (122) oder die Gleichungen (123), (123ª) erfüllt sein, aus denen durch Division die andere:

$$\zeta' = \frac{\lambda\zeta + \mu}{\nu\zeta + \varrho}$$

hervorgeht, welche ζ, ζ' als zwei „einander äquivalente“ Zahlen bezeichnet.

18. Von den Kongruenzen mit beliebigen Idealmoduln wenden wir uns jetzt im besonderen zu solchen mit Primidealmoduln. Einige einfache Bemerkungen mögen noch voraufgeschickt werden.

Jedes Ideal $\mathfrak{m}$ enthält positive rationale ganze Zahlen, da, wenn μ irgend eine in $\mathfrak{m}$ enthaltene und von Null verschiedene Zahl ist, stets auch $\pm N(\mu)$ darin vorhanden ist. Unter allen diesen positiven ganzen Zahlen ist eine die kleinste, sie heiße m. Dann muß jede andere in $\mathfrak{m}$ enthaltene rationale ganze Zahl m' durch m teilbar sein; denn sonst wäre $m' = qm + r$, wo r positiv und kleiner wäre als m, und mit m und m' wäre auch $r = m' - qm$ in $\mathfrak{m}$ enthalten, gegen die Bedeutung von m. Ist also m die kleinste positive ganze Zahl eines Ideals $\mathfrak{m}$, so bildet die Gesamtheit aller in $\mathfrak{m}$ enthaltenen rationalen Zahlen den Modulus $[m]$.

Wenn das Ideal $\mathfrak{m}$ zu einer rationalen ganzen Zahl k, d. h. zum Ideale $\mathfrak{g}k$ relativ prim ist, so ist auch die Zahl m prim gegen k. In der Tat, nach (95) ist

$$(\mathfrak{m} + \mathfrak{g}k) \cdot (\mathfrak{m} - \mathfrak{g}k) = \mathfrak{m} \cdot \mathfrak{g}k$$

oder, da nach Voraussetzung $\mathfrak{m} + \mathfrak{g}k = \mathfrak{g}$ ist:

$$\mathfrak{m} - \mathfrak{g}k = \mathfrak{m} \cdot k.$$

Ist nun d der größte gemeinsame Teiler der Zahlen m und k, so ist ihr kleinstes gemeinsames Vielfache gleich $\frac{mk}{d}$ und dieses sowohl in $\mathfrak{m}$ als in $\mathfrak{g}k$, mithin auch in

$$\mathfrak{m} - \mathfrak{g}k = \mathfrak{m} \cdot k$$

enthalten. Da hiernach $\frac{m}{d}$ in $\mathfrak{m}$ enthalten sein müßte, folgt $d = 1$, wie behauptet.

Unter der gleichen Voraussetzung ist auch $\mathfrak{N}(\mathfrak{m})$ relativ prim zu k. Da nämlich m in $\mathfrak{m}$ enthalten ist, so gilt das Gleiche vom Ideale $\mathfrak{g}m$, und folglich gibt es ein Ideal $\mathfrak{j}$, für welches $\mathfrak{g}m = \mathfrak{m} \cdot \mathfrak{j}$, mithin

$$\mathfrak{N}(\mathfrak{g}m) = N(m) = m^n$$

teilbar ist durch $\mathfrak{N}(\mathfrak{m})$. Weil dem vorigen Satze zufolge m prim ist gegen k, muß es also $\mathfrak{N}(\mathfrak{m})$ auch sein.

Bedeutet nun $\mathfrak{p}$ ein Primideal, so muß die kleinste in ihm vorhandene rationale Zahl p eine gewöhnliche Primzahl sein. Denn, wäre $p = q \cdot r$ das Produkt zweier von 1 verschiedenen ganzen Zahlen, so wäre das Ideal

$$\mathfrak{g}p = \mathfrak{g}q \cdot \mathfrak{g}r;$$

weil es aber in $\mathfrak{p}$ enthalten oder durch $\mathfrak{p}$ teilbar ist, müßte auch einer der Faktoren $\mathfrak{g}q$, $\mathfrak{g}r$, etwa $\mathfrak{g}q$ teilbar durch $\mathfrak{p}$, also $q < p$ in $\mathfrak{p}$ enthalten sein, gegen die Bedeutung von p. Diese kleinste in $\mathfrak{p}$ vorhandene rationale Zahl p ist aber auch die einzige darin enthaltene Primzahl, denn jede andere in $\mathfrak{p}$ enthaltene rationale Zahl ist ja dem zuvor Bewiesenen zufolge ein Vielfaches von $\mathfrak{p}$. Somit ist die rationale Primzahl p des Primideales $\mathfrak{p}$ eine eindeutig bestimmte und mag daher die ihm zugehörige Primzahl heißen. Da das Ideal $\mathfrak{g}p$ in $\mathfrak{p}$ enthalten ist, besteht eine Gleichung von der Form

$$\mathfrak{g}p = \mathfrak{p} \cdot \mathfrak{j},$$

worin auch $\mathfrak{j}$ ein Ideal ist; und aus ihr ergibt sich $\mathfrak{N}(\mathfrak{p})$ als ein Teiler von $\mathfrak{N}(\mathfrak{g}p) = N(p) = p^n$, also ebenfalls als eine Potenz von p:

$$\mathfrak{N}(\mathfrak{p}) = p^f. \tag{124}$$

Der durch diese Gleichung definierte Exponent f soll der *Grad des Primideals* $\mathfrak{p}$ genannt werden.

Doch ist hiermit seine volle Bedeutung für die Theorie noch nicht genügend bezeichnet. Wir leiten vielmehr noch weitere Definitionen desselben ab. Mehrere Zahlen $\gamma', \gamma'', \cdots, \gamma^{(m)}$ in $\mathfrak{g}$ mögen (mod. $\mathfrak{p}$) unabhängig heißen, falls eine Zahl

$$r'\gamma' + r''\gamma'' + \cdots + r^{(m)}\gamma^{(m)}, \tag{125}$$

in welcher die $r^{(i)}$ rationale ganze Zahlen bedeuten, nur dann in $\mathfrak{p}$ enthalten sein kann, wenn alle $r^{(i)}$ Zahlen in $\mathfrak{p}$, d. h. wenn sie sämtlich Vielfache von p sind. Ist im Gegenteil die Zahl (125) mit nicht durchweg durch p teilbaren Koeffizienten $r^{(i)}$ in $\mathfrak{p}$ enthalten, d. i. besteht die Kongruenz

$$r'\gamma' + r''\gamma'' + \cdots + r^{(m-1)}\gamma^{(m-1)} + r^{(m)}\gamma^{(m)} \equiv 0 \text{ (mod. } \mathfrak{p}),$$

so wird, wenn z. B. $r^{(m)}$ durch p nicht aufgeht, $\gamma^{(m)}$ einer homogenen linearen Funktion der übrigen $\gamma^{(i)}$ kongruent sein; denn, ist $s^{(m)}$ der Socius von $r^{(m)}$ (mod. p), derart, daß

$$r^{(m)} \cdot s^{(m)} - 1$$

teilbar ist durch p und folglich enthalten in $\mathfrak{p}$, so ergibt sich

aus der obigen Kongruenz durch Multiplikation mit $s^{(m)}$ eine andere von der Gestalt

$$s'\gamma' + s''\gamma'' + \cdots + s^{(m-1)}\gamma^{(m-1)} \equiv \gamma^{(m)} \pmod{\mathfrak{p}}.$$

Dies vorausgeschickt, seien $\gamma_1, \gamma_2, \cdots, \gamma_n$ beliebige Basiszahlen von $\mathfrak{g}$. Da das Primideal $\mathfrak{p}$ von $\mathfrak{g}$ verschieden ist, können sie nicht alle in $\mathfrak{p}$ enthalten sein; gehört also etwa γ_1 dem Ideale $\mathfrak{p}$ nicht an, so wird man, mit γ_1 zunächst eine, dann zwei, dann drei usw. der übrigen Basiszahlen verbindend, eine gewisse Anzahl von (mod. $\mathfrak{p}$) unabhängigen derselben, etwa die f Zahlen $\gamma_1, \gamma_2, \cdots, \gamma_f$ feststellen können, derart, daß eine Kongruenz

$$(126) \qquad r_1\gamma_1 + r_2\gamma_2 + \cdots + r_f\gamma_f \equiv 0 \pmod{\mathfrak{p}}$$

nur bestehen kann, wenn sämtliche r_i durch p teilbar sind, jede der übrigen Basiszahlen $\gamma_{f+1}, \cdots, \gamma_n$ aber linear mit ganzzahligen Koeffizienten (mod. $\mathfrak{p}$) durch jene f ersten ausdrückbar ist. Es wird behauptet, daß diese Anzahl f der voneinander unabhängigen Basiszahlen eine eindeutig bestimmte, nämlich mit dem Grade des Primideales $\mathfrak{p}$ identisch ist.

In der Tat, da jede Zahl γ in $\mathfrak{g}$ die Form hat

$$(127) \qquad \gamma = \varrho_1\gamma_1 + \varrho_2\gamma_2 + \cdots + \varrho_n\gamma_n,$$

worin die ϱ_i ganze rationale Zahlen, die Zahlen $\gamma_{f+1}, \cdots, \gamma_n$ aber (mod. $\mathfrak{p}$) linear durch die übrigen ausdrückbar sind, so wird stets

$$(128) \qquad \gamma \equiv r_1\gamma_1 + r_2\gamma_2 + \cdots + r_f\gamma_f \pmod{\mathfrak{p}}$$

mit ganzzahligen r_i gesetzt werden können. Zwei solche Zahlen

$$\gamma' = r_1'\gamma_1 + r_2'\gamma_2 + \cdots + r_f'\gamma_f$$
$$\gamma'' = r_1''\gamma_1 + r_2''\gamma_2 + \cdots + r_f''\gamma_f$$

werden jedoch dann und nur dann (mod. $\mathfrak{p}$) kongruent sein, wenn ihre Differenz

$$(r_1' - r_1'')\gamma_1 + (r_2' - r_2'')\gamma_2 + \cdots + (r_f' - r_f'')\gamma_f$$

in $\mathfrak{p}$ enthalten, d. h. die sämtlichen Differenzen $r_i' - r_i''$ durch p teilbar sind. Daher gibt der Ausdruck (128) nur genau soviel (mod. $\mathfrak{p}$) inkongruente Zahlen γ, als man erhält, indem man jeden der f Koeffizienten r_i die p Glieder eines voll-

ständigen Restsystems (mod. p) durchlaufen läßt, d. i. p^f. Da man aber die Anzahl der (mod. $\mathfrak{p}$) inkongruenten Zahlen in $\mathfrak{g}$ mit $\mathfrak{N}(\mathfrak{p})$ bezeichnet, so ergibt sich die Gleichung (124) und damit die Identität der Anzahl f mit dem durch diese Gleichung definierten Grade des Primideals $\mathfrak{p}$. Zugleich sieht man ein, daß die Formel (128), wenn die r_i vollständige Restsysteme (mod p) durchlaufen, sämtliche Klassen (mod. $\mathfrak{p}$) repräsentiert oder ein vollständiges Restsystem der Zahlen in $\mathfrak{g}$ (mod. $\mathfrak{p}$) liefert.

Mit Bezug auf eine spätere Gelegenheit mag darauf hingewiesen werden, daß bei dieser Betrachtung $\mathfrak{p}$ nur als ein Idealteiler von p, nicht gerade als Primidealteiler vorauszusetzen nötig ist.

19. Eine einzige der gedachten p^f Zahlen γ ist kongruent Null (mod. $\mathfrak{p}$), d. i. in $\mathfrak{p}$ enthalten, diejenige nämlich, bei welcher sämtliche r_i durch p teilbar sind; alle übrigen sind daher relativ prim zu $\mathfrak{p}$; wir bezeichnen sie, zur Abkürzung

$$p^f = \pi \tag{129}$$

setzend, mit $\gamma', \gamma'', \cdots, \gamma^{(\pi-1)}$. Ist dann γ irgend eine zu $\mathfrak{p}$ relativ prime Zahl, so sind es auch (vgl. die Sätze in Nr. 11) die Produkte

$$\gamma\gamma', \gamma\gamma'', \cdots, \gamma\gamma^{(\pi-1)}, \tag{130}$$

welche zudem (mod. $\mathfrak{p}$) inkongruent sind, da eine Kongruenz

$$\gamma\gamma^{(i)} \equiv \gamma\gamma^{(k)} \pmod{\mathfrak{p}}$$

auf die Gleichung

$$\mathfrak{g}\gamma \cdot \mathfrak{g}(\gamma^{(i)} - \gamma^{(k)}) = \mathfrak{p} \cdot \mathfrak{j},$$

in welcher $\mathfrak{j}$ ein Ideal bedeutet, hinauskommt, während doch kein Faktor der linken Seite durch $\mathfrak{p}$ teilbar ist. Demnach repräsentieren die in $\mathfrak{g}$ enthaltenen Zahlen (130) ein vollständiges Restsystem von $\mathfrak{g}$ (mod. $\mathfrak{p}$) und müssen in ihrer Gesamtheit also den Zahlen $\gamma^{(i)}$ (mod. $\mathfrak{p}$) kongruent sein. Daraus folgt dann (Anfang von Nr. 15) auch die Kongruenz

$$\gamma\gamma' \cdot \gamma\gamma'' \cdots \gamma\gamma^{(\pi-1)} \equiv \gamma'\gamma'' \cdots \gamma^{(\pi-1)} \pmod{\mathfrak{p}},$$

welche einer Gleichung von der Form

$$\mathfrak{g}(\gamma^{\pi-1} - 1) \cdot \mathfrak{g}\gamma' \cdots \mathfrak{g}\gamma^{(\pi-1)} = \mathfrak{p} \cdot \mathfrak{j}$$

gleichbedeutend ist und die Folgerung nach sich zieht, daß

$\mathfrak{g}(\gamma^{\pi-1}-1)$ durch $\mathfrak{p}$ teilbar, d. h. $\gamma^{\pi-1}-1$ eine in $\mathfrak{p}$ enthaltene Zahl oder

$$\gamma^{\pi-1}\equiv 1 \pmod{\mathfrak{p}}$$

ist. Man erhält also nachstehenden Satz, das hier geltende Analogon des einfachen Fermatschen Satzes:

Jede durch $\mathfrak{p}$ nicht teilbare Zahl γ in $\mathfrak{g}$ erfüllt die Bedingung

$$\gamma^{p^f-1}\equiv 1 \pmod{\mathfrak{p}}. \tag{131}$$

Da hieraus

$$\gamma^{p^f}\equiv \gamma \pmod{\mathfrak{p}} \tag{132}$$

gefolgert wird, andererseits diese Kongruenz aber auch für jede in $\mathfrak{p}$ enthaltene Zahl γ besteht, darf man diesen „Fermatschen Satz“ auch in der erweiterten Weise zum Ausdrucke bringen, daß man sagt: Für *jede* Zahl γ in $\mathfrak{g}$ findet die Kongruenz (132) statt.

Wie der einfache *Fermat*sche Satz der gewöhnlichen Zahlentheorie, so läßt sich auch dieser *Fermat*sche Satz der Idealtheorie verallgemeinern, nämlich von Primidealmoduln auf beliebige Moduln ausdehnen. Nach (131) ist

$$\gamma^{\pi-1}=1+\beta,$$

wo β eine Zahl in $\mathfrak{p}$ bedeutet. Erhebt man diese Gleichung zur π^{ten} Potenz, so kommt

$$\gamma^{\pi(\pi-1)}=1+\pi\cdot\beta+\frac{\pi(\pi-1)}{1\cdot 2}\cdot\beta^2+\cdots+\beta^\pi;$$

bedenkt man aber, daß $\pi=N(\mathfrak{p})$ eine Zahl in $\mathfrak{p}$, also $\pi\cdot\beta$ eine Zahl in $\mathfrak{p}\cdot\mathfrak{p}$, und daß die höheren Potenzen von β gleichfalls solche Zahlen sind, so kann vorstehende Gleichung einfacher geschrieben werden in der Form:

$$\gamma^{\pi(\pi-1)}=1+\beta',$$

wo β' dem Ideale $\mathfrak{p}^2$ angehört. Hieraus folgt

$$\gamma^{\pi^2(\pi-1)}=1+\pi\cdot\beta'+\frac{\pi(\pi-1)}{1\cdot 2}\cdot\beta'^2+\cdots+\beta'^\pi,$$

wo nun $\pi\cdot\beta'$ dem Ideale $\mathfrak{p}\cdot\mathfrak{p}^2$, die höheren Potenzen von β' aber sogar dem Ideale $\mathfrak{p}^2\cdot\mathfrak{p}^2$ angehören, folglich ist

$$\gamma^{\pi^2(\pi-1)}=1+\beta'',$$

unter β'' eine Zahl des Ideals $\mathfrak{p}^3$ verstanden. Fährt man so fort, so gelangt man ersichtlich zu der Kongruenz

$$\gamma^{\pi^{a-1}(\pi-1)} \equiv 1 \pmod{\mathfrak{p}^a},$$

der man auch die Form geben kann

$$\gamma^{\varphi(\mathfrak{p}^a)} \equiv 1 \pmod{\mathfrak{p}^a}; \tag{133}$$

dabei bezeichnet γ irgend eine durch $\mathfrak{p}$ nicht teilbare Zahl in $\mathfrak{g}$. Ist nun wieder $\mathfrak{j}$ das Ideal

$$\mathfrak{j} = \mathfrak{p}^a \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

und γ eine zu ihm relativ prime, also durch keins der Primideale $\mathfrak{p}, \mathfrak{p}_1, \cdots, \mathfrak{p}_r$ teilbare Zahl, so bestehen neben der Kongruenz (133) die folgenden analogen:

$$\mathfrak{p}^{\varphi(\mathfrak{p}_1^{a_1})} \equiv 1 \pmod{\mathfrak{p}_1^{a_1}}$$
$$\cdots\cdots\cdots$$
$$\gamma^{\varphi(\mathfrak{p}_r^{a_r})} \equiv 1 \pmod{\mathfrak{p}_r^{a_r}}$$

und daher offenbar die Kongruenz

$$\gamma^{\varphi(\mathfrak{j})} \equiv 1$$

für jeden der relativ primen Moduln $\mathfrak{p}^a, \mathfrak{p}_1^{a_1}, \cdots, \mathfrak{p}_r^{a_r}$, d. h. die Zahl $\gamma^{\varphi(\mathfrak{j})} - 1$ ist in jedem dieser Moduln und daher auch in ihrem kleinsten gemeinsamen Vielfachen $\mathfrak{j}$ enthalten. Demnach gilt der Satz: Für jede zum Ideale $\mathfrak{j}$ relativ prime Zahl γ in $\mathfrak{g}$ besteht die Kongruenz

$$\gamma^{\varphi(\mathfrak{j})} \equiv 1 \pmod{\mathfrak{j}}. \tag{134}$$

20. Doch, zu den Kongruenzen zurückkehrend, deren Moduln Primideale sind, beweisen wir vor allem einen allgemeinen Kongruenzsatz über die mögliche Anzahl ihrer Wurzeln. Sei

$$F(x) = \alpha^0 \cdot x^r + \alpha' \cdot x^{r-1} + \cdots + \alpha^{(r)} \tag{135}$$

eine ganze Funktion von x, deren Koeffizienten ganze Zahlen des Körpers sind. Ist γ eine Zahl in $\mathfrak{g}$, für welche $F(\gamma)$ dem Ideale $\mathfrak{p}$ angehört, so soll γ eine Wurzel der Kongruenz

$$F(x) \equiv 0 \pmod{\mathfrak{p}} \tag{136}$$

genannt werden; sind alle Koeffizienten in (135) Zahlen des Ideals $\mathfrak{p}$, so wird jede Zahl γ in $\mathfrak{g}$ dieser Kongruenz genügen und daher soll sie dann eine identische heißen. Der gemeinte

Satz besagt nun: **Eine nicht identische Kongruenz (136) kann nicht mehr inkongruente Wurzeln in $\mathfrak{g}$ haben, als ihr Grad beträgt, wenn der Modulus ein Primideal ist.** Hierbei verstehen wir unter dem Grade der Kongruenz den Exponenten der höchsten in $F(x)$ auftretenden Potenz von x, deren Koeffizient eine nicht in $\mathfrak{p}$ enthaltene Zahl ist. Hätte nämlich die Kongruenz (136) vom Grade r mehr als r inkongruente Wurzeln, so seien

$$\gamma, \gamma_1, \gamma_2, \cdots, \gamma_r$$

$r+1$ solche. Von ihnen erfüllen dann die letzten r auch die Kongruenz

$$F(x) - \alpha^0 \cdot (x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_r) \equiv 0 \pmod{\mathfrak{p}},$$

welche höchstens noch vom $r-1^{\text{ten}}$ Grade ist und deren Koeffizienten ganze Zahlen des Körpers sind. Setzt man also voraus, der Satz gelte für alle Kongruenzen, deren Grad kleiner als r, so müßte vorstehende Kongruenz identisch und demnach auch für $x=\gamma$ erfüllt sein, woraus, da nach Voraussetzung $F(\gamma)\equiv 0 \pmod{\mathfrak{p}}$, sich

$$\alpha^0(\gamma-\gamma_1)(\gamma-\gamma_2)\cdots(\gamma-\gamma_r) \equiv 0 \pmod{\mathfrak{p}}$$

ergäbe, eine unmögliche Kongruenz, weil den Annahmen zufolge kein Faktor des Produktes durch $\mathfrak{p}$ teilbar ist. Hiernach gilt der Satz für Kongruenzen r^{ten} Grades, wenn er für solche geringeren Grades, und somit allgemein, wenn er für Kongruenzen ersten Grades gilt. Solche lassen sich aber schreiben, wie folgt:

$$\gamma x \equiv \gamma^{(h)} \pmod{\mathfrak{p}},$$

worin γ eine nicht in $\mathfrak{p}$ enthaltene Zahl in $\mathfrak{g}$, $\gamma^{(h)}$ eine Zahl der Reihe $\gamma', \gamma'', \cdots, \gamma^{(\pi-1)}$ oder die Null bedeutet; im erstern Falle gibt es eine bestimmte Zahl $\gamma^{(i)}$ derselben Reihe, für welche $\gamma\gamma^{(i)} \equiv \gamma^{(h)}$ ist, d. h. $x \equiv \gamma^{(i)}$ ist eine Wurzel der Kongruenz, andernfalls ergibt sich $x \equiv 0$; aber es gibt auch keine zweite Wurzel, da für zwei inkongruente Lösungen $x \equiv \alpha'$, $x \equiv \alpha''$ sich $\gamma(\alpha'-\alpha'') \equiv 0$ ergäbe, was nicht sein kann. **Kongruenzen ersten Grades (mod. $\mathfrak{p}$) haben mithin stets eine, aber nur eine einzige Wurzel.**

Der so bewiesene allgemeine Kongruenzsatz läßt nun erkennen, daß die Anzahl f der (mod. $\mathfrak{p}$) unabhängigen Basis-

zahlen von $\mathfrak{g}$ die kleinste Zahl von der Beschaffenheit ist, daß für jede Zahl in $\mathfrak{g}$ die Kongruenz besteht

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}}.$$

Diese Kongruenz findet nach voriger Nummer für jede solche Zahl γ tatsächlich statt. Bestünde nun im Gegenteil, wenn $f' < f$ ist, für alle Zahlen γ in $\mathfrak{g}$ auch die Kongruenz

$$\gamma^{p^{f'}} \equiv \gamma \pmod{\mathfrak{p}},$$

so hätte diese Kongruenz sämtliche $\mathfrak{N}(\mathfrak{p}) = p^f$ inkongruente Zahlen γ zu Wurzeln, also mehr inkongruente Wurzeln als ihr Grad beträgt, dem gedachten Satze zuwider. Oder auch so: Wenn f die kleinste Zahl ist, für welche sämtliche Zahlen γ in $\mathfrak{g}$ die Kongruenz

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}} \tag{137}$$

erfüllen, so sind unter den Basiszahlen von $\mathfrak{g}$ genau f unabhängig (mod. $\mathfrak{p}$); denn, betrüge diese Anzahl im Gegenteil f', so wäre $\mathfrak{N}(\mathfrak{p}) = p^{f'}$ die Anzahl aller (mod. $\mathfrak{p}$) inkongruenten Zahlen in $\mathfrak{g}$, welche alle nach der Voraussetzung die Kongruenz (137) erfüllen; sie erfüllen aber nach dem Fermatschen Satze dann auch die Kongruenz

$$\gamma^{p^{f'}} \equiv \gamma \pmod{\mathfrak{p}};$$

nach der Bedeutung von f wäre also $f \leqq f'$, dem allgemeinen Kongruenzsatze zufolge aber $f \geqq f'$, also ist $f = f'$. So ergibt sich die dritte Bedeutung des Exponenten f in (124): der Grad des Primideals $\mathfrak{p}$ ist die kleinste Zahl von der Beschaffenheit, daß für alle Zahlen γ in $\mathfrak{g}$ die Kongruenz

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}}$$

besteht.

Eine noch andere Bedeutung des Grades von $\mathfrak{p}$ erkennt man mittels folgender Bemerkungen. Aus der Kongruenz (128) folgt durch ihre Erhebung zur p^{ten} Potenz, wenn man bedenkt, daß jedes Vielfache von p eine Zahl in $\mathfrak{p}$, $r_i^p - r_i$ aber für jede rationale ganze Zahl r_i ein solches Vielfache ist, die andere:

$$\gamma^p \equiv r_1\gamma_1^p + r_2\gamma_2^p + \cdots + r_f\gamma_f^p \pmod{\mathfrak{p}},$$

und wenn diese wieder zur p^{ten} Potenz erhoben und so fortgefahren wird, entsteht die folgende Reihe von f Kongruenzen:

$$\left.\begin{array}{l} \gamma \equiv r_1\gamma_1 + r_2\gamma_2 + \cdots + r_f\gamma_f \\ \gamma^p \equiv r_1\gamma_1^p + r_2\gamma_2^p + \cdots + r_f\gamma_f^p \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \gamma^{p^{f-1}} \equiv r_1\gamma_1^{p^{f-1}} + r_2\gamma_2^{p^{f-1}} + \cdots + r_f\gamma_f^{p^{f-1}} \end{array}\right\} \pmod{\mathfrak{p}},$$

deren Determinante

$$\Gamma = \begin{vmatrix} \gamma_1 & \gamma_2 \cdots\cdots & \gamma_f \\ \gamma_1^p & \gamma_2^p \cdots\cdots & \gamma_f^p \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \gamma_1^{p^{f-1}} & \gamma_2^{p^{f-1}} \cdots & \gamma_f^{p^{f-1}} \end{vmatrix}$$

nicht durch $\mathfrak{p}$ teilbar sein kann, denn sonst erhielte man (vgl. Kap. 1, Nr. 7) aus ihnen eine Kongruenz von der Form

$$\alpha\gamma^{p^{f-1}} + \alpha_1\gamma^{p^{f-2}} + \cdots + \alpha_{f-1}\gamma^p + \alpha_f\gamma \equiv 0,$$

deren Koeffizienten ganze, nicht sämtlich in $\mathfrak{p}$ enthaltene Zahlen des Körpers sind, und welche für jede der $\mathfrak{N}(\mathfrak{p}) = p^f \pmod{\mathfrak{p}}$ inkongruenten Zahlen γ erfüllt sein müßte, entgegen dem allgemeinen Kongruenzsatze dieser Nummer, da ihr Grad nur p^{f-1} beträgt. Bildet man nun die Matrix

$$(138) \qquad \begin{array}{llll} \gamma_1, & \gamma_2, & \cdots\cdots, & \gamma_n \\ \gamma_1^p, & \gamma_2^p, & \cdots\cdots, & \gamma_n^p \\ \cdot & \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \gamma_1^{p^{n-1}}, & \gamma_2^{p^{n-1}}, & \cdots, & \gamma_n^{p^{n-1}}, \end{array}$$

so wird die aus ihren n^2 Elementen gebildete Determinante entweder durch $\mathfrak{p}$ teilbar oder durch $\mathfrak{p}$ nicht teilbar sein. Im letzteren Falle verstehe man unter r die Zahl n, im ersteren Falle die bestimmte Zahl von der Beschaffenheit, daß alle Unterdeterminanten größeren als r^{ten} Grades durch $\mathfrak{p}$ teilbar, unter denjenigen r^{ten} Grades aber mindestens eine durch $\mathfrak{p}$ nicht teilbar ist. Die so bestimmte Zahl heiße der **Rang** der Determinante oder der **Matrix** (138). Wir wollen zeigen, daß dieser Rang nichts anderes als der Grad des Primideals $\mathfrak{p}$ ist. Denn die voraufgeschickte Bemerkung lehrt, daß, wenn f dieser Grad ist, eine der Unterdeterminanten f^{ten} Grades durch

$\mathfrak{p}$ nicht teilbar ist. Andererseits müssen dann alle Unterdeterminanten $f+1^{\text{ten}}$ Grades und somit auch die aus ihnen in linearer Weise gebildeten Unterdeterminanten höheren Grades durch $\mathfrak{p}$ teilbar sein; in der Tat darf man, wenn es sich nur um Teilbarkeit durch $\mathfrak{p}$ handelt, in jeder Reihe der Matrix:

$$\gamma_1^{p^h},\ \gamma_2^{p^h},\ \cdots,\ \gamma_n^{p^h}$$

wegen (137) den Exponenten h auf seinen kleinsten, nicht negativen Rest (mod. f) reduzieren; eine aus mehr als f Reihen der Matrix gebildete Determinante enthielte dann notwendig zwei (mod. $\mathfrak{p}$) kongruente Reihen und würde also kongruent Null (mod. $\mathfrak{p}$) d. i. teilbar durch $\mathfrak{p}$ sein.

Demnach läßt sich schließlich der Grad des Primideals $\mathfrak{p}$ auch als der Rang der aus den Basiszahlen von $\mathfrak{g}$ gebildeten Matrix (138) definieren.

21. Auf den Ergebnissen der letzten Nummern erbaut sich nun eine Theorie der höheren Kongruenzen (mod. $\mathfrak{p}$), welche der in Kap. 3 (mod. p) gegebenen völlig analog ist und bei deren Darstellung wir deshalb uns kurz fassen können. Der Grund dieser Analogie aber ist einfach der, daß die letztere Theorie nur einen speziellen Fall der auf Primidealmoduln bezüglichen bildet. Bezeichnen wir, um dies einzusehen, wie in Kap. 3, Nr. 4, mit $P(x)$ eine (mod. p) primäre irreduktible Funktion n^{ten} Grades und mit α eine Wurzel der irreduktibeln Gleichung $P(x)=0$, und nennen $\mathfrak{K}$ den von dieser Wurzel erzeugten Körper. Ist dann $\gamma_1, \gamma_2, \cdots, \gamma_n$ eine Basis für die Gesamtheit $\mathfrak{g}$ seiner ganzen Zahlen, so bestehen, da α eine solche ist, n ganzzahlige Gleichungen von der Form:

$$(139)\qquad \begin{aligned} 1 &= r_{01}\gamma_1 + r_{02}\gamma_2 + \cdots\cdots\cdots + r_{0n}\gamma_n \\ \alpha &= r_{11}\gamma_1 + r_{12}\gamma_2 + \cdots\cdots\cdots + r_{1n}\gamma_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha^{n-1} &= r_{n-1,1}\gamma_1 + r_{n-1,2}\gamma_2 + \cdots + r_{n-1,n}\gamma_n, \end{aligned}$$

deren Determinante R durch p nicht teilbar sein kann, da sonst nach Kap. 1, Nr. 7 sich rationale ganze, nicht sämtlich durch p teilbare Zahlen $\varrho_0, \varrho_1, \cdots, \varrho_{n-1}$ würden angeben lassen derart, daß für die Zahl α eine Kongruenz

$$\varrho_{n-1}\alpha^{n-1} + \varrho_{n-2}\alpha^{n-2} + \cdots + \varrho_1\alpha + \varrho_0 \equiv 0 \pmod{p}$$

stattfände, der vorausgesetzten Irreduktibilität der Funktion $P(x) \pmod{p}$ zuwider. Da nun aus den Gleichungen (139) jedes der Produkte $\mathrm{R}\gamma_i$ und somit auch für jede ganze Zahl γ des Körpers $\mathfrak{K}$, da sie durch die Formel

$$\gamma = r_1\gamma_1 + r_2\gamma_2 + \cdots + r_n\gamma_n$$

ausdrückbar ist, das Produkt $\mathrm{R}\gamma$ in der Form

$$a + a'\alpha + a''\alpha^2 + \cdots + a^{(n-1)}\cdot\alpha^{n-1}$$

dargestellt werden kann, so erhält man durch Multiplikation mit dem Sozius von R (mod. p) eine Kongruenz, wie sie folgt:

$$(140) \quad \gamma \equiv a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \pmod{p},$$

welche zeigt, daß die ganzen Zahlen des Körpers mit den Zahlen ω des Bereichs G_α, die wir an der angeführten Stelle des dritten Kapitels in Betracht gezogen, (mod. p) identisch sind, oder auch, daß die Potenzen $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ zur irreduktibeln Basis des Ideals $\mathfrak{g}$ (mod. p) gewählt werden können. Hieraus erkennt man zunächst leicht, daß das Ideal $\mathfrak{p} = \mathfrak{g}p$ des betrachteten Körpers $\mathfrak{K}$ ein Primideal ist. In der Tat, wäre $\mathfrak{p}$ zusammengesetzt: $\mathfrak{p} = \mathfrak{q}\cdot\mathfrak{r}$, wo $\mathfrak{q}$, $\mathfrak{r}$ zwei von $\mathfrak{g}$ verschiedene Ideale sind, so gäbe es eine Zahl λ in $\mathfrak{q}$, welche nicht in $\mathfrak{p}$ enthalten ist, da sonst $\mathfrak{q} \succ \mathfrak{p} \succ \mathfrak{q}$, also $\mathfrak{q} = \mathfrak{p}$ und $\mathfrak{r} = \mathfrak{g}$ wäre gegen die Voraussetzung; ebenso gibt es eine Zahl μ in $\mathfrak{r}$, welche nicht in $\mathfrak{p}$ enthalten ist, das Produkt $\lambda\mu$ beider Zahlen aber würde in $\mathfrak{p}$ sein. Dies ist indessen leicht als unzulässig nachzuweisen. Denn, setzt man

$$\left.\begin{aligned} \lambda \equiv q(\alpha), \quad \mu \equiv r(\alpha) \\ \text{also} \qquad \lambda\mu \equiv q(\alpha)\cdot r(\alpha) \end{aligned}\right\} \pmod{p},$$

wo $q(\alpha)$, $r(\alpha)$ zwei Ausdrücke von der Gestalt (140) sind, so würde aus

$$\lambda\mu \equiv 0 \pmod{\mathfrak{p}}$$

d. h. (mod. p) nach Kap. 3, Nr. 4 die Funktionenkongruenz

$$q(x)\cdot r(x) \equiv 0 \pmod{p,\ P(x)}$$

hervorgehen, der zufolge einer der Faktoren, etwa $q(x)$, kongruent Null sein müßte, was wieder mit

$$\lambda \equiv q(\alpha) \equiv 0 \pmod{p}$$

oder (mod. $\mathfrak{p}$) identisch, also der Voraussetzung zuwider sein würde. Der Grad dieses Primideals $\mathfrak{p} = \mathfrak{g}p$ ist n, da die Anzahl der (mod. p) inkongruenten ganzen Zahlen des betrachteten Körpers oder der inkongruenten Ausdrücke von der Form (140) gleich p^n gefunden wird. — Aus diesen Punkten leuchtet ein, daß die Betrachtung der Zahlen des Bereiches G_α (mod. p) nur als besonderer Fall in derjenigen der ganzen Zahlen eines Körpers in bezug auf einen Primidealmodulus beschlossen ist, und in der Tat finden sich im wesentlichen die dort gegebenen Sätze auch in der allgemeineren Theorie.

Ist nämlich $\mathfrak{p}$ irgend ein Primideal des Körpers $K(\mathsf{A}; R)$, so besteht für jede ganze algebraische Zahl γ des letzteren die Kongruenz

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}},$$

welche das Analogon der durch jede Zahl ω des Bereichs G_α erfüllten Kongruenz

$$\omega^{p^n} \equiv \omega \pmod{p}$$

darstellt. Zugleich gilt, wie gezeigt worden, der allgemeine Satz über die mögliche Anzahl von Wurzeln einer Kongruenz nach einem Primzahlmodulus p auch in bezug auf einen Primidealmodulus $\mathfrak{p}$. Ferner gilt auch das Analogon des zweiten Hilfssatzes in Nr. 5 des 3. Kapitels in Gestalt folgenden Satzes:

Ist $F(x)$ eine ganze, ganzzahlige Funktion von x, und γ eine ganze algebraische Zahl des Körpers, welche der Kongruenz

$$F(x) \equiv 0 \pmod{\mathfrak{p}} \tag{141}$$

Genüge leistet, so erfüllen die letzteren sämtliche Potenzen

$$\gamma,\ \gamma^p,\ \gamma^{p^2},\ \gamma^{p^3},\ \cdots\cdot \tag{142}$$

In der Tat besteht dem ersten Hilfssatze jener Nummer zufolge die Kongruenz

$$F(x)^p \equiv F(x^p) \pmod{p},$$

d. i. eine Gleichung von der Form

$$F(x)^p = F(x^p) + p \cdot \Phi(x),$$

wo $\Phi(x)$ eine ganze, ganzzahlige Funktion von x bedeutet. Aus ihr ergibt sich für $x = \gamma$, da $\Phi(\gamma)$ zugleich mit γ eine ganze Zahl des Körpers bezeichnet, jedes Vielfache von p aber im Ideale $\mathfrak{p}$ enthalten ist, die Kongruenz

$$F(\gamma)^p \equiv F(\gamma^p) \quad (\text{mod. } \mathfrak{p})$$

und, da nach Voraussetzung $F(\gamma) \equiv 0$ (mod. $\mathfrak{p}$) ist, folgt auch, wie behauptet,

$$F(\gamma^p) \equiv 0 \quad (\text{mod. } \mathfrak{p}),$$

d. h. γ^p und daher dann auch $\gamma^{p^2}, \gamma^{p^3}, \cdots$ sind Wurzeln der Kongruenz (141).

Endlich bemerken wir noch, daß eine ganze, ganzzahlige Funktion $F(x)$ stets gleichzeitig nach den beiden Moduln p und $\mathfrak{p}$ irreduktibel ist. Denn, wären auch $F_1(x)$, $F_2(x)$ ganze, ganzzahlige Funktionen, so ergäbe sich aus der Kongruenz entsprechender Zahlenkoeffizienten in $F(x)$ und in $F_1(x) \cdot F_2(x)$ nach dem Modulus p auch diejenige nach dem Idealteiler $\mathfrak{p}$ von p als Modulus; umgekehrt aber, wenn diese Koeffizienten (mod. $\mathfrak{p}$) kongruent, d. i. ihre Differenz in $\mathfrak{p}$ enthalten ist, so ist sie als ganze rationale Zahl durch p teilbar, die Koeffizienten sind mithin auch (mod. p) kongruent. Demnach wäre stets gleichzeitig (mod. p) und (mod. $\mathfrak{p}$)

$$F(x) \equiv F_1(x) \cdot F_2(x).$$

Auf Grund dieser Umstände ergeben sich nun die folgenden, denen des 3. Kapitels entsprechenden Sätze durch völlig übereinstimmende Erwägungen.

Jede durch $\mathfrak{p}$ nicht teilbare Zahl γ in $\mathfrak{g}$ gehört zu einem bestimmten Exponenten $\delta > 0$ derart, daß γ^δ die niedrigste Potenz von γ ist, für welche

$$\gamma^\delta \equiv 1 \quad (\text{mod. } \mathfrak{p})$$

ist; dieser Exponent ist ein Teiler von $p^f - 1$. Zu jedem Teiler δ von $p^f - 1$ gehören, wenn $\varphi(\delta)$ die Eulersche Funktion der gewöhnlichen Zahlentheorie bezeichnet, $\varphi(\delta)$ inkongruente Zahlen γ. Demnach gibt es $\varphi(p^f - 1)$ inkongruente

Zahlen ϱ, welche zum Exponenten p^f-1 gehören; diese mögen *Primitivzahlen* (mod. $\mathfrak{p}$) heißen. Sie haben die Eigenschaft, daß die p^f-1 Potenzen

$$(143)\qquad \varrho,\ \varrho^2,\ \varrho^3,\ \cdots,\ \varrho^{p^f-1}$$

(mod. $\mathfrak{p}$) inkongruent sind, da aus einer Kongruenz

$$\varrho^h \equiv \varrho^k \pmod{\mathfrak{p}} \atop (h<k<p^f)$$

schon $\varrho^{k-h}\equiv 1$ (mod. $\mathfrak{p}$) hervorginge, während doch $k-h<p^f-1$ ist; die p^f-1 ersten Potenzen (143) einer Primitivzahl ϱ stellen daher ein vollständiges Restsystem der durch $\mathfrak{p}$ nicht teilbaren Zahlen in $\mathfrak{g}$ (mod. $\mathfrak{p}$) dar.

Ebenso paßt jede durch $\mathfrak{p}$ nicht teilbare Zahl γ zu einem bestimmten Exponenten $d>0$ derart, daß p^d die niedrigste Potenz von p ist, für welche

$$\gamma^{p^d}\equiv\gamma \pmod{\mathfrak{p}}$$

wird; dieser Exponent ist ein Teiler von f. Zu jedem Teiler d von f passen $g(d)$ Zahlen γ, wo $g(d)$ denselben Ausdruck bedeutet, wie er durch die Formeln (72) und (63) des 3. Kapitels bestimmt worden ist. Die Anzahl $g(1)$ der zum Exponenten 1 passenden Zahlen beträgt hiernach p; in der Tat erfüllen diese Zahlen die Kongruenz

$$\gamma^p\equiv\gamma \pmod{\mathfrak{p}},$$

deren Wurzeln aber auch umgekehrt nur zum Exponenten 1 passen können. Da dieselbe Kongruenz nicht mehr als p inkongruente Wurzeln haben kann, die p inkongruenten Zahlen $0, 1, 2, \cdots, p-1$ ihr aber genügen, muß jede Zahl γ, welche der Kongruenz

$$x^p\equiv x \pmod{\mathfrak{p}}$$

genügt, einer ganzen rationalen Zahl kongruent sein. Betrachten wir z. B. die Determinante Γ in Nr. 20. Erhebt man diese zur p^{ten} Potenz, so ergibt sich mit Beachtung des Fermatschen Satzes (137) leicht die Kongruenz

$$\Gamma^p\equiv\begin{vmatrix}\gamma_1^p, & \gamma_2^p, & \cdots, & \gamma_f^p\\ \gamma_1^{p^2}, & \gamma_2^{p^2}, & \cdots, & \gamma_f^{p^2}\\ \cdot & \cdot & \cdot & \cdot\\ \gamma_1, & \gamma_2, & \cdots, & \gamma_f\end{vmatrix},$$

eine Determinante, die sich von Γ nur um das entgegengesetzte Vorzeichen unterscheiden kann. Daher wird gewiß immer

$$(\Gamma^2)^p \equiv \Gamma^2$$

und folglich Γ^2 nach dem eben Bemerkten einer rationalen ganzen Zahl (mod. $\mathfrak{p}$) kongruent sein.

Ferner erkennt man, wie in Nr. 7 des 3. Kapitels, daß die ganze Klasse der zu einem Teiler d von f passenden Zahlen γ, welche nicht durch $\mathfrak{p}$ teilbar sind, aus den Klassen der Zahlen zusammengesetzt ist, die zu den, dem Ausdrucke p^d-1 eigenen Teilern δ_d', δ_d'', $\cdots$ gehören. Die Klasse der zu einem solchen Teiler $\delta_d^{(i)}$ gehörigen Zahlen zerfällt aber wieder in $\frac{\varphi\left(\delta_d^{(i)}\right)}{d}$ Unterabteilungen von je d Zahlen, die einer (mod. $\mathfrak{p}$) irreduktibeln, ganzzahligen Kongruenz

$$P_d(x) \equiv 0 \pmod{\mathfrak{p}}$$

d^{ten} Grades Genüge leisten. Um daher den Ausdruck

$$x^{p^f} - x \tag{144}$$

(mod. $\mathfrak{p}$) in seine irreduktibeln Faktoren zu zerlegen, bestimme man sämtliche Teiler d von f, für jeden derselben die der Zahl p^d-1 eigenen Teiler $\delta_d^{(i)}$, und für jeden der letzteren die $\frac{\varphi\left(\delta_d^{(i)}\right)}{d}$ irreduktibeln ganzzahligen Funktionen $P_d(x)$, welche den gedachten Unterabteilungen entsprechen. Das Produkt aller so gebildeten Funktionen, noch mit x multipliziert, ist dann dem Ausdrucke (144) (mod. $\mathfrak{p}$) kongruent und stellt dessen Zerlegung in seine (mod. $\mathfrak{p}$) irreduktibeln, ganzzahligen Faktoren dar. (Vgl. K. Hensel, J. f. Math. 101, p. 99.)

22. Da die Primitivzahlen ϱ (mod. $\mathfrak{p}$) zum Exponenten p^f-1 gehören, so werden sie zum Exponenten f passen, denn, paßten sie zu einem von f verschiedenen Teiler d von f, so wäre schon $\varrho^{p^d} \equiv \varrho$, mithin, da ϱ nicht teilbar ist durch $\mathfrak{p}$, schon $\varrho^{p^d-1} \equiv 1$ (mod. $\mathfrak{p}$), gegen die Bedeutung von ϱ. Den letzten Bemerkungen der vorigen Nummer zufolge verteilen sich daher die $\varphi(p^f-1)$ Primitivzahlen auf $\frac{\varphi(p^f-1)}{f}$ verschiedene irreduktible ganzzahlige Funktionen f^{ten} Grades als deren Wurzeln, und es genügt demnach jede Primitivzahl (mod. $\mathfrak{p}$)

einer (mod. p) irreduktibeln ganzzahligen Kongruenz f^{ten} Grades.

Sei aber $P(x)$ eine zunächst beliebige (mod. p) irreduktible ganzzahlige Funktion, m ihr Grad und ϱ irgend eine Wurzel der Kongruenz

$$(145) \qquad P(x) \equiv 0 \pmod{\mathfrak{p}}$$

d. i. eine im Körper $K(\mathsf{A};\, R)$ enthaltene ganze Zahl, für welche $P(\varrho)$ im Ideale $\mathfrak{p}$ enthalten ist.

Man erkennt zunächst ganz ähnlich wie in Kap. 3, Nr. 4, daß, wenn $F(x)$ irgendeine andere ganze, ganzzahlige Funktion von x ist, die Zahlenkongruenz

$$(146) \qquad F(\varrho) \equiv 0 \pmod{\mathfrak{p}}$$

völlig gleichbedeutend ist mit der Funktionenkongruenz

$$(147) \qquad F(x) \equiv 0 \quad \text{mod.} \{p,\ P(x)\}.$$

In der Tat, wenn die letztere stattfindet, so gibt es ganze, ganzzahlige Funktionen $\varphi(x)$, $\psi(x)$ von x von der Beschaffenheit, daß

$$F(x) = p \cdot \varphi(x) + P(x) \cdot \psi(x)$$

ist; für $x = \varrho$ sind $P(\varrho)$, $\varphi(\varrho)$, $\psi(\varrho)$ ganze Zahlen des Körpers, die erste derselben ebenso wie p in $\mathfrak{p}$ enthalten, also folgt aus vorstehender Gleichung

$$F(\varrho) \equiv 0 \pmod{\mathfrak{p}}.$$

Besteht aber umgekehrt die Kongruenz (146), so muß $F(x)$ kongruent Null sein mod. $\{p,\ P(x)\}$, denn sonst wäre $F(x)$ (mod. p) relativ prim zu $P(x)$, folglich bestünde eine Kongruenz von der Gestalt

$$F(x) \cdot \varphi_1(x) + P(x) \cdot \varphi_2(x) \equiv 1 \pmod{p},$$

in welcher $\varphi_1(x)$, $\varphi_2(x)$ ganze, ganzzahlige Funktionen, also $\varphi_1(\varrho)$, $\varphi_2(\varrho)$ ganze Zahlen des Körpers bedeuten, aus der sich also für $x = \varrho$ wegen $P(\varrho) \equiv 0$, $F(\varrho) \equiv 0 \pmod{\mathfrak{p}}$ die unmögliche Kongruenz

$$0 \equiv 1 \pmod{\mathfrak{p}}$$

ergäbe.

Da nun eine Kongruenz (147) nicht stattfinden kann,

wenn $F(x)$ geringeren Grades ist wie $P(x)$, es sei denn, daß $F(x) \equiv 0 \pmod{p}$, d. h. die Koeffizienten von $F(x)$ durch p teilbar sind, so sind die m Potenzen

$$1, \varrho, \varrho^2, \cdots, \varrho^{m-1}$$

(mod. $\mathfrak{p}$) unabhängige Zahlen, nämlich eine Kongruenz

$$F(\varrho) = r_0 + r_1\varrho + r_2\varrho^2 + \cdots + r_{m-1}\varrho^{m-1} \equiv 0 \pmod{\mathfrak{p}}$$

mit rational ganzzahligen Koeffizienten nur möglich, wenn sie sämtlich in $\mathfrak{p}$ enthalten, d. h. durch p teilbar sind. Hieraus leuchtet ein, daß jede ganze, ganzzahlige Funktion $F(\varrho)$ von ϱ einem und auch nur einem Ausdrucke von der Form

$$F(\varrho) \equiv a_0 + a_1\varrho + a_2\varrho^2 + \cdots + a_{m-1}\varrho^{m-1} \pmod{\mathfrak{p}},$$

in welchem die Koeffizienten a_i Zahlen der Reihe $0, 1, 2, \cdots, p-1$ sind, kongruent und daß daher p^m die Anzahl der Klassen sein wird, in welche alle Funktionen $F(\varrho)$ sich (mod. $\mathfrak{p}$) verteilen.

Ist insbesondere $P(x)$ eine (mod. p) irreduktible Funktion vom Grade f des Primideals $\mathfrak{p}$, so *gibt* es eine Wurzel ϱ der Kongruenz (145); denn $P(x)$ ist (Kap. 3) nach dem Modulus p also auch nach dem Modulus $\mathfrak{p}$ ein Faktor des Ausdrucks (144) und dieser hat dem Fermatschen Satze zufolge p^f Wurzeln, die sich derart auf seine Faktoren verteilen, daß jeder der letzteren genau so viel Wurzeln erhält, als sein Grad beträgt. Hiernach sind in diesem Falle die f Potenzen

$$1, \varrho, \varrho^2, \cdots, \varrho^{f-1} \tag{148}$$

(mod. $\mathfrak{p}$) unabhängige Zahlen, und eine Kongruenz von der Gestalt

$$F(\varrho) = r_0 + r_1\varrho + r_2\varrho^2 + \cdots + r_{f-1}\varrho^{f-1} \equiv 0 \pmod{\mathfrak{p}} \tag{149}$$

mit rational ganzzahligen Koeffizienten nicht anders möglich, als wenn diese sämtlich durch p teilbar sind. Nun bestehen aber nach (128) f Kongruenzen von der Form:

$$\begin{aligned} 1 &\equiv r_{01}\gamma_1 + r_{02}\gamma_2 + \cdots + r_{0f}\gamma_f \\ \varrho &\equiv r_{11}\gamma_1 + r_{12}\gamma_2 + \cdots + r_{1f}\gamma_f \\ &\cdots\cdots\cdots\cdots \\ \varrho^{f-1} &\equiv r_{f-1,1}\gamma_1 + r_{f-1,2}\gamma_2 + \cdots + r_{f-1,f}\gamma_f \end{aligned} \pmod{\mathfrak{p}}, \tag{150}$$

deren ganzzahlige Determinante R dem eben Gesagten zufolge nicht durch $\mathfrak{p}$, d. i. durch p teilbar sein kann, da sonst f ganze rationale, nicht sämtlich durch p teilbare Zahlen $r_0, r_1, \cdots, r_{f-1}$ vorhanden sein würden, der Art, daß

$$r_0 + r_1\varrho + \cdots + r_{f-1}\varrho^{f-1} \equiv 0 \pmod{\mathfrak{p}}$$

stattfinden würde, und es ergibt sich somit aus den Kongruenzen (150) für jede Zahl γ in $\mathfrak{g}$ eine Kongruenz

$$\mathrm{R}\gamma \equiv a + a'\varrho + \cdots + a^{(f-1)}\varrho^{f-1} \pmod{\mathfrak{p}}.$$

Bezeichnet aber R′ den Socius von R (mod. p), sodaß die Kongruenz $\mathrm{RR}' \equiv 1$ (mod. p), also auch (mod. $\mathfrak{p}$) erfüllt ist, so wird die vorstehende Kongruenz durch Multiplikation mit R′ in die folgende Gestalt

$$(151) \qquad \gamma \equiv a_0 + a_1\varrho + \cdots + a_{f-1}\varrho^{f-1} \pmod{\mathfrak{p}}$$

übergeführt, in welcher die a_i rationale ganze Zahlen sind, die zudem als kleinste positive Reste (mod. p) vorausgesetzt werden können. Jede ganze Zahl γ des Körpers ist also (mod. $\mathfrak{p}$) einem, und nach dem über die Kongruenz (149) Bemerkten auch nur einem einzigen Ausdrucke (151) von dieser Beschaffenheit kongruent, was aufs neue bestätigt, daß die Anzahl der (mod. $\mathfrak{p}$) inkongruenten Zahlen des Körpers p^f beträgt.

Diese Resultate gelten gewiß, wenn ϱ eine Primitivzahl (mod. $\mathfrak{p}$), da unter $P(x) \equiv 0$ (mod. $\mathfrak{p}$) die Kongruenz verstanden werden kann, der eine solche, wie bemerkt, genügt.

Möglicherweise kann aber die Zahl $P(\varrho)$, welche durch das Primideal $\mathfrak{p}$ aufgeht, noch eine höhere Potenz von $\mathfrak{p}$ als Faktor enthalten; doch kann die Wurzel ϱ der Kongruenz (145) so gewählt werden, daß dies nicht der Fall, daß also $P(\varrho)$ zwar durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist. Wäre nämlich ϱ_0 eine solche Wurzel der Kongruenz, daß $P(\varrho_0)$ noch durch $\mathfrak{p}^2$ aufgeht, so setze man

$$\varrho = \varrho_0 + \beta,$$

wo β eine in $\mathfrak{p}$, aber nicht in $\mathfrak{p}^2$ enthaltene Zahl bezeichnet; man bemerke, daß, wenn ϱ_0 eine Primitivzahl (mod. $\mathfrak{p}$) wäre, das gleiche auch von ϱ gälte, da für jeden positiven ganzen

Exponenten k sich

$$\varrho^k \equiv \varrho_0{}^k \pmod{\mathfrak{p}}$$

ergibt. Da nun

$$P(\varrho) = P(\varrho_0 + \beta) = P(\varrho_0) + \beta \cdot P'(\varrho_0) + \beta^2 \cdot \frac{P''(\varrho_0)}{1 \cdot 2} + \cdots$$

gesetzt werden kann, wo die Koeffizienten der Potenzen von β ganze, ganzzahlige Funktionen von ϱ_0, d. h. ganze Zahlen des Körpers sind, so folgt aus den Annahmen

$$(152) \qquad P(\varrho) \equiv \beta \cdot P'(\varrho_0) \pmod{\mathfrak{p}^2}.$$

In dieser Kongruenz ist der erste Faktor β zur Rechten durch $\mathfrak{p}$ aber nicht durch $\mathfrak{p}^2$, der zweite Faktor $P'(\varrho_0)$ nicht durch $\mathfrak{p}$ teilbar; denn dieser ist ein Ausdruck $f-1^{\text{ten}}$ Grades in ϱ_0, also, falls er durch $\mathfrak{p}$ teilbar, von der Form $p \cdot f(\varrho_0)$, d. h. es müßten, wenn

$$P(x) = x^f + c_1 x^{f-1} + \cdots + c_{f-1} x + c_f$$

gedacht wird, in

$$P'(x) = f x^{f-1} + c_1(f-1) x^{f-2} + \cdots + c_{f-1}$$

sämtliche Koeffizienten durch p teilbar oder $P'(x) \equiv 0 \pmod{p}$ sein, was in Kap. 3, Nr. 3 als unzulässig nachgewiesen worden ist. So schließt man endlich aus der Kongruenz (152), daß $P(\varrho)$ zwar durch $\mathfrak{p}$ aber nicht mehr durch $\mathfrak{p}^2$ teilbar ist, die Zahl ϱ also eine Wurzel der Kongruenz (145) von der Beschaffenheit ist, wie sie nachgewiesen werden sollte.

Diese Feststellung ist von Bedeutung für den Fall, daß man von Kongruenzen (mod. $\mathfrak{p}$) zu solchen (mod. $\mathfrak{p}^m$) überzugehen veranlaßt ist. Es kann nämlich jetzt folgender Satz bewiesen werden:

Jede ganze Zahl des Körpers ist einer ganzen, ganzzahligen Funktion der eben bestimmten Zahl ϱ (mod. $\mathfrak{p}^m$) kongruent. Zum Beweise bilde man den Ausdruck

$$(153) \qquad \alpha_0 + \alpha_1 P(\varrho) + \alpha_2 P(\varrho)^2 + \cdots + \alpha_{m-1} P(\varrho)^{m-1}.$$

Läßt man in demselben jeden der m Koeffizienten α_i ein vollständiges Restsystem (mod. $\mathfrak{p}$) durchlaufen, indem man

$$\alpha_i = a_{i0} + a_{i1}\varrho + \cdots + a_{i,f-1}\varrho^{f-1}$$

setzt und den Koeffizienten a_{ik} alle Werte $0, 1, 2, \cdots, p-1$ beilegt, so erhält man, da α_i auf solche Weise p^f Werte an-

nimmt, im ganzen p^{mf} Werte des Ausdrucks (153), welche, wie nun gezeigt werden soll, (mod. $\mathfrak{p}^m$) inkongruent sind. Wären nämlich zwei solcher Werte:

$$(154) \qquad \begin{cases} \alpha_0' + \alpha_1' P(\varrho) + \cdots + \alpha_{m-1}' P(\varrho)^{m-1} \\ \alpha_0'' + \alpha_1'' P(\varrho) + \cdots + \alpha_{m-1}'' P(\varrho)^{m-1} \end{cases}$$

(mod. $\mathfrak{p}^m$) also auch (mod. $\mathfrak{p}$) kongruent, so ergäbe sich aus dem Umstande, daß $P(\varrho)$ teilbar ist durch $\mathfrak{p}$, die Kongruenz

$$\alpha_0' \equiv \alpha_0'' \pmod{\mathfrak{p}},$$

eine Bedingung, welche notwendig die Gleichheit der beiden Zahlen α_0', α_0'' nach sich zieht. Die Kongruenz der beiden Werte (154) (mod. $\mathfrak{p}^m$) lieferte also, da $P(\varrho)$ durch $\mathfrak{p}$, aber nicht durch eine höhere Potenz von $\mathfrak{p}$ teilbar ist, die Kongruenz der folgenden Werte

$$\begin{aligned} &\alpha_1' + \alpha_2' P(\varrho) + \cdots + \alpha_{m-1}' P(\varrho)^{m-2} \\ &\alpha_1'' + \alpha_2'' P(\varrho) + \cdots + \alpha_{m-1}'' P(\varrho)^{m-2} \end{aligned}$$

(mod. $\mathfrak{p}^{m-1}$), woraus wieder $\alpha_1' = \alpha_1''$ hervorgehen würde usw., bis die völlige Identität der Ausdrücke (154) sich herausstellte. Da hiernach die p^{mf} Werte des Ausdrucks (153) in der Tat (mod. $\mathfrak{p}^m$) inkongruent sind, und $p^{mf} = \mathfrak{N}(\mathfrak{p}^m)$ die Anzahl aller (mod. $\mathfrak{p}^m$) inkongruenten Zahlen in $\mathfrak{g}$ bezeichnet, so muß, wie der Satz behauptet, jede ganze Zahl γ des Körpers einem jener Ausdrücke, d. i. einer ganzen, ganzzahligen Funktion von ϱ (mod. $\mathfrak{p}^m$) kongruent sein.

Offenbar darf in diesem Satze an Stelle von ϱ irgend eine andere Zahl ϱ' genommen werden, welche (mod. $\mathfrak{p}^2$) mit ϱ kongruent ist, denn aus $\varrho' \equiv \varrho \pmod{\mathfrak{p}^2}$ folgt $P(\varrho') \equiv P(\varrho)$ (mod. $\mathfrak{p}^2$) und folglich ist $P(\varrho')$ wie $P(\varrho)$ teilbar durch $\mathfrak{p}$ aber nicht durch $\mathfrak{p}^2$, ein Umstand, welcher den behaupteten Satz zur Folge hatte. Man bemerke zudem, daß, falls ϱ als Primitivzahl (mod. $\mathfrak{p}$) gedacht war, auch ϱ' eine solche verbleiben wird.

Nun setze man, da $\mathfrak{g}p$ durch $\mathfrak{p}$ teilbar ist,

$$\mathfrak{g}p = \mathfrak{p}^m \cdot \mathfrak{q},$$

wo $\mathfrak{q}$ ein Ideal ist, welches durch das Primideal $\mathfrak{p}$ nicht mehr aufgeht. Dann gibt es, da sonst $\mathfrak{q} \succ \mathfrak{p}$ wäre, eine Zahl γ in

$\mathfrak{q}$, welche nicht in $\mathfrak{p}$ also auch nicht in $\mathfrak{p}^2$ enthalten ist. Dem verallgemeinerten Fermatschen Satze zufolge ist also

$$\gamma^{p^f(p^f-1)} \equiv 1 \pmod{\mathfrak{p}^2},$$

folglich, wenn man das Produkt $\varrho' \cdot \gamma^{p^f(p^f-1)}$ kurz wieder ϱ nennt,

$$(155) \qquad \varrho \equiv \varrho' \pmod{\mathfrak{p}^2}.$$

Da in der (mod. p) irreduktibeln Funktion $P(x)$ das konstante Glied nicht durch p, also als rationale ganze Zahl auch durch kein in p aufgehendes Primideal teilbar sein kann, so muß es zu $\mathfrak{q}$ relativ prim sein, während die übrigen Glieder des Ausdrucks $P(\varrho)$, da γ und folglich auch ϱ in $\mathfrak{q}$ enthalten ist, durch $\mathfrak{q}$ teilbar sind. Daraus folgt, daß $P(\varrho)$ selbst relativ prim gegen $\mathfrak{q}$ ist, und da es andererseits teilbar ist durch $\mathfrak{p}$ aber nicht durch $\mathfrak{p}^2$, so muß der größte gemeinsame Teiler von

$$\mathfrak{g}P(\varrho) \quad \text{und} \quad \mathfrak{g}p$$

gleich $\mathfrak{p}$ sein. So findet sich endlich der folgende wichtige Satz:

Ist $\mathfrak{p}$ ein Primideal f^{ten} Grades und $P(x)$ eine beliebige der Primfunktionen (mod. p) von eben demselben Grade, so gibt es eine Wurzel ϱ der letzteren von der Beschaffenheit, daß jede ganze Zahl des Körpers in bezug auf eine beliebig hohe Potenz $\mathfrak{p}^m$ als Modulus einer ganzen, ganzzahligen Funktion von ϱ kongruent, und daß zugleich $\mathfrak{p}$ der größte gemeinsame Teiler der beiden Hauptideale $\mathfrak{g}p$ und $\mathfrak{g}P(\varrho)$ ist, in Zeichen:

$$(156) \qquad \mathfrak{p} = \{p, P(\varrho)\}.$$

Man darf hinzufügen, daß bei geeigneter Wahl der Primfunktion $P(x)$ die Zahl ϱ als Primitivzahl gedacht werden darf.

Durch diesen Satz wird das allgemeine Ergebnis der Nr. 17, nach welchem jedes Ideal größter gemeinsamer Teiler zweier Hauptideale ist, für den Fall eines Primideales durch die dann für die Hauptideale geltende Beziehung zu der irreduktibeln Kongruenz f^{ten} Grades $P(x) \equiv 0 \pmod{\mathfrak{p}}$ wesentlich schärfer gefaßt und vertieft.

Siebentes Kapitel.

Von den Diskriminantenteilern.

1. Nächst dem Grade eines endlichen Körpers $\mathfrak{K}$ ist eine seiner wesentlichsten arithmetischen Bestimmungen die Grundzahl oder Diskriminante desselben. Wir verstanden unter der Grundzahl

$$\mathrm{D} = \Delta(\mathfrak{g})$$

des Körpers die Diskriminante irgend einer Basis $\gamma_1, \gamma_2, \cdots, \gamma_n$ des Ideals $\mathfrak{g}$; da solche Basis stets zugleich eine Basis des Körpers ist, so ist die Grundzahl immer eine von Null verschiedene und zwar ganze rationale Zahl (s. Kap. 1, Nr. 8 und Kap. 4, Nr. 3). Sind nun

$$\gamma_i' = c_{1i}\gamma_1 + c_{2i}\gamma_2 + \cdots + c_{ni}\gamma_i \qquad (1)$$
$$(i = 1, 2, \cdots, n)$$

irgend welche n Zahlen in $\mathfrak{g}$, so besteht (Kap. 1, (51)) die Beziehung

$$\Delta(\gamma_1', \gamma_2', \cdots, \gamma_n') = |c_{ik}|^2 \cdot \Delta(\mathfrak{g}),$$

und somit werden die n Zahlen γ_i' eine Basis des Körpers bilden oder nicht, jenachdem die Determinante $|c_{ik}|$ von Null verschieden oder gleich Null ist. Wenn aber θ irgend eine ganze Zahl des Körpers ist, so bestehen n Gleichungen von der Form

$$\theta^i = c_{1i}\gamma_1 + c_{2i}\gamma_2 + \cdots + c_{ni}\gamma_n, \qquad (2)$$
$$(i = 0, 1, 2, \cdots, n-1)$$

denen zufolge, wenn ihre Determinante $|c_{ik}|$ zur Abkürzung mit C bezeichnet und als Index der Zahl θ benannt wird,

$$\Delta(1, \theta, \theta^2, \cdots, \theta^{n-1}) = C^2 \cdot \Delta(\mathfrak{g}) \qquad (3)$$

ist, und dem Gesagten gemäß werden die Potenzen

$$1, \theta, \theta^2, \cdots, \theta^{n-1}$$

dann und nur dann eine Basis des Körpers, d. h. θ eine den letztern erzeugende Zahl n^{ten} Grades oder eine Zahl der dem Körper $\mathfrak{K}$ entsprechenden Gattung $\mathfrak{G}$ sein, wenn der Index C von θ von Null verschieden ist. Man denke sich sämtliche Zahlen θ der Gattung $\mathfrak{G}$; der Gleichung (3) gemäß

ist die Grundzahl D des Körpers gemeinsamer Teiler, jede in D aufgehende rationale Primzahl also ein gemeinsamer Primteiler der Diskriminanten aller dieser Zahlen. Jede einzelne Diskriminante aber kann noch besondere Primteiler haben, diejenigen nämlich, welche im Index der Zahl θ enthalten sind; diese letzteren sind von Kronecker „außerwesentliche Teiler" genannt worden im Gegensatze zu den in D aufgehenden „wesentlichen Teilern"; wir möchten den Ausdruck „individuelle Teiler" für sie angemessener finden, denn diese „außerwesentlichen" Primteiler spielen im Gegenteile in gewisser Hinsicht eine sehr wesentliche Rolle. In der Tat hat zuerst Dedekind den Nachweis geliefert, daß, wenn p eine Primzahl ist, welche nicht im Index von θ aufgeht, ihre Zerlegung in Primidealfaktoren des Körpers $\mathfrak{K}$ aus der Gleichung, welcher θ genügt, mit Hilfe der Theorie der höheren Kongruenzen gefunden werden kann, während für Primfaktoren des Index dies nicht gleicherweise möglich ist. Wenn nämlich

$$F(x) = 0 \tag{4}$$

die irreduktible Gleichung ist, welcher θ genügt, und die ganze, ganzzahlige Funktion $F(x)$ ist, in irreduktible Faktoren (mod. p) zerlegt,

$$F(x) \equiv P_1(x)^{a_1} P_2(x)^{a_2} \cdots P_r(x)^{a_r} \pmod{p},$$

so entspricht dieser Zerlegung im ersteren Falle eine Zerlegung

$$p = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_r^{a_r}$$

der Primzahl p in Primideale $\mathfrak{p}_i$, welche mit den Primfunktionen $P_i(x)$ eng verknüpft und gleichen Grades sind, wie sie; im andern Falle fehlt eine solche notwendige Konformität der Zerlegungen. Mit dieser Erkenntnis wurde zugleich der Grund aufgedeckt, warum die früheren Bemühungen, die Kummersche, auf die Kongruenz $F(x) \equiv 0 \pmod{p}$ gegründete Theorie der idealen Zahlen, welche für die aus Einheitswurzeln gebildeten Zahlenkörper erfolgreich gewesen, auf jede Art von Zahlenkörpern auszudehnen, von vornherein aussichtslos sein mußten; denn, falls eine Primzahl p etwa in dem Index einer jeden Zahl θ der Gattung $\mathfrak{G}$ enthalten sein sollte, so könnte keine einzige der entsprechenden Gleichungen (4) benutzt

werden, um mittels Zerlegung der Funktion $F(x)$ (mod. p) nach der Theorie der höheren Kongruenzen die Zerlegung von p in seine Primidealfaktoren zu gewinnen, und so müßte die Begründung dieser Zerlegung innerhalb des gedachten Zahlenkörpers auf jene Theorie notwendig dann lückenhaft bleiben. Daß es aber Körper gibt, in denen der Fall solcher Primzahlen p sich wirklich ereignet, dafür wurde an einem Beispiele gleichfalls von Dedekind zuerst der Beweis erbracht.[1])

Indessen haben neuere Untersuchungen den Weg gewiesen, wie dennoch die Theorie der höheren Kongruenzen zur Grundlage für die Zerlegung sämtlicher Primzahlen p in ihre Idealfaktoren verwendbar gemacht werden kann. Dies Verdienst gebührt Hensel, welcher, gestützt zwar auf Kroneckersche Grundsätze und Vorarbeiten, über die Resultate dieses Forschers, sie ergänzend oder weiterführend, wesentlich hinausgegangen ist.[2]) Das Prinzip seiner Untersuchungen ist das gleiche, dessen sich Kronecker bedient hat: statt der algebraischen Zahlen selbst Formen zu betrachten, deren Koeffizienten derartige Zahlen sind, und durch solche Assoziation neuer Größengebilde oder das methodische Hilfsmittel der unbestimmten Koeffizienten „das Gebiet der algebraischen Größen genügend zu erweitern, um den bei ganzen Zahlen und bei ganzen rationalen Funktionen von Variabeln geltenden einfachen Gesetzen der Teilbarkeit, welche beim Übergange zu den ganzen algebraischen Größen modifiziert werden, wiederum Raum zur vollen Wirksamkeit zu schaffen.“[3]) Bevor wir dazu übergehen können, von den Henselschen Arbeiten eine Darstellung zu geben, müssen wir in betreff der Kroneckerschen „Formen“ einige Vorbemerkungen machen, auf die auch später zurückzugreifen sein wird.

---

1) S. zu diesem allen Dedekind „über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen“, Götting. Abh. 23. Bd., 1878; Götting. Anz. 1871, p. 1488.

2) Hensel „Untersuchung der Fundamentalgleichung einer Gattung“, Journ. f. Math. 113, p. 61, und „arithmetische Untersuch. üb. die gemeinsamen außerwesentlichen Diskriminantenteiler einer Gattung“, ebendas. p. 128.

3) Kronecker, Festschrift „Grundzüge einer arithmetischen Theorie der algebraischen Größen“, s. auch Journ. f. Math. 92, p. 48.

2. Mittels der in der 2ten und 3ten Nummer des dritten Kapitels entwickelten Grundsätze überzeugt man sich leicht, daß eben dieselben Entwicklungen auch Gültigkeit behalten, falls statt der ganzen, ganzzahligen Funktionen einer Veränderlichen solche Funktionen mehrerer Veränderlichen in Betracht gezogen werden. Sie gelten somit auch für ganze Funktionen einer Veränderlichen x, deren Koeffizienten, statt ganze Zahlen zu sein, ganze, ganzzahlige Funktionen von beliebig viel Unbestimmten $u, v, \cdots$ sind. Ist also

$$\mathrm{F}(x;\, u, v, \cdots)$$

eine solche Funktion und wird eine andere Funktion

$$\Phi(x;\, u, v, \cdots)$$

derselben Art ein Teiler der ersteren (mod. p) genannt, wenn es eine dritte Funktion $\Psi(x;\, u, v, \cdots)$ von gleicher Art gibt so beschaffen, daß

$$(5)\qquad \mathrm{F}(x;\, u, v, \cdots) \equiv \Phi(x;\, u, v, \cdots)\cdot \Psi(x;\, u, v, \cdots) \pmod{p}$$

ist, d. h. daß die Koeffizienten gleicher Potenzen von x auf beiden Seiten (mod. p) kongruente Funktionen von $u, v, \cdots$ sind, so erhält man ganz die gleichen Teilbarkeitssätze, wie sie an der angegebenen Stelle für ganze, ganzzahlige Funktionen einer Veränderlichen bewiesen worden sind. Heißen z. B. zwei Funktionen

$$\mathrm{F}_1(x;\, u, v, \cdots),\quad \mathrm{F}_2(x;\, u, v, \cdots)$$

ohne gemeinsamen Teiler (mod. p), wenn sie keinen andern Teiler gemeinsam haben, als etwa eine in allen ihren Koeffizienten aufgehende rationale ganze Zahl oder ganze, ganzzahlige Funktion nur von den Unbestimmten $u, v, \cdots$, so wird es stets zwei andere ganze Funktionen

$$\Phi_1(x;\, u, v, \cdots),\quad \Phi_2(x;\, u, v, \cdots)$$

geben von der Beschaffenheit, daß eine Beziehung

$$(6)\qquad \mathrm{F}_1(x; u, v, \cdots)\cdot \Phi_1(x; u, v, \cdots) + \mathrm{F}_2(x; u, v, \cdots)\cdot \Phi_2(x; u, v, \cdots) \equiv C(u, v, \cdots) \pmod{p}$$

stattfindet, in welcher die rechte Seite eine ganze, ganzzahlige Funktion der Unbestimmten $u, v, \cdots$ allein bedeutet. Wir nennen ferner $\mathrm{F}(x;\, u, v, \cdots)$ eine Primfunktion (mod. p),

wenn eine Zerlegung derselben nach der Formel (5) nur in der Weise möglich ist, daß von den Faktoren zur Rechten der eine eine ganze Zahl oder ganze, ganzzahlige Funktion der Unbestimmten $u, v, \cdots$ allein, der andere nur um einen ebensolchen Faktor von F verschieden ist; präziser denken wir uns die Primfunktion stets primär, d. h. ihren höchsten Koeffizienten der Einheit gleich. Alsdann gilt wieder der fundamentale Satz, daß das Produkt zweier ganzen Funktionen nur dann durch eine Primfunktion (mod. p) teilbar ist, wenn es einer der Faktoren ist, wodurch dann weiter begründet ist, daß jede ganze Funktion auf eine einzige Weise als Produkt von primären Primfunktionen (mod. p) dargestellt werden, nämlich eine Kongruenz

$$(7)\quad F(x; u, v, \cdots) \equiv C(u, v, \cdots) \cdot P_1(x; u, v, \cdots)^{a_1} \cdots P_h(x; u, v, \cdots)^{a_h} \pmod{p}$$

aufgestellt werden kann, in welcher $C(u, v, \cdots)$ eine ganze, ganzzahlige Funktion allein von den Unbestimmten, die Funktionen $P_1, \cdots, P_h$ aber verschiedene Primfunktionen (mod. p) in endlicher Anzahl bezeichnen.

3. Andererseits denken wir uns eine ganze Funktion $F(u, v, \cdots)$ der Unbestimmten $u, v, \cdots$, deren Koeffizienten $\alpha_1, \alpha_2, \cdots, \alpha_r$ beliebige ganze Zahlen eines endlichen Körpers $\mathfrak{K}$ sind; nach Kronecker heißt man sie „eine Form des Körpers“ mit den Unbestimmten $u, v, \cdots$. Jeder Form des Körpers entspricht ein bestimmtes Ideal desselben, nämlich das aus ihren Koeffizienten entspringende Ideal

$$(8)\qquad \mathfrak{a} = \{\alpha_1, \alpha_2, \cdots, \alpha_r\};$$

umgekehrt gibt es zu jedem Ideale des Körpers Formen, denen es entspricht, denn, bedeuten $\varphi_1, \varphi_2, \cdots, \varphi_r$ irgendwelche, aber verschieden aus Potenzen von $u, v, \cdots$ gebildete Produkte, so ist

$$F(u, v, \cdots) = \alpha_1\varphi_1 + \alpha_2\varphi_2 + \cdots + \alpha_r\varphi_r$$

eine solche Form. Das Ideal $\mathfrak{a}$, welches der Form $F(u, v, \cdots)$ entspricht, heiße der *Inhalt* derselben.[1])

1) Hilbert, Bericht über die Theorie der algebraischen Zahlkörper, im Jahresber. der Deutschen Math. Vereinigung, 4. Bd., 1894/95, p. 187.

Hier gilt nun der folgende fundamentale Satz: **Der Inhalt eines Produkts von Formen ist gleich dem Produkte aus den Inhalten seiner Faktoren.** Es genügt, ihn für ein Produkt zweier Faktoren zu beweisen. Seien also $F_1(u, v, \cdots)$, $F_2(u, v, \cdots)$ zwei Funktionen mit den Inhalten

$$\mathfrak{a}' = \{\alpha_1', \alpha_2', \cdots, \alpha'_{r'}\}, \quad \mathfrak{a}'' = \{\alpha_1'', \alpha_2'', \cdots, \alpha''_{r''}\}$$

und der Inhalt ihres Produktes

$$F(u, v, \cdots) = F_1(u, v, \cdots) \cdot F_2(u, v, \cdots) \tag{9}$$

sei

$$\mathfrak{a} = \{\alpha_1, \alpha_2, \cdots, \alpha_r\}.$$

Macht man wieder, indem man die positive ganze Zahl g groß genug wählt, wie in Kap. 6, Nr. 6 ausgeführt worden ist, die Substitution

$$u = x, \; v = x^g, \; w = x^{g^2}, \cdots,$$

so gehen die drei in der Formel (9) enthaltenen Funktionen in Funktionen von x über, welche durch

$$\begin{aligned} F(x) &= \beta_1 x^{h_1} + \beta_2 x^{h_2} + \cdots + \beta_r x^{h_r} \\ F_1(x) &= \beta_1' x^{h_1'} + \beta_2' x^{h_2'} + \cdots + \beta'_{r'} x^{h'_{r'}} \\ F_2(x) &= \beta_1'' x^{h_1''} + \beta_2'' x^{h_2''} + \cdots + \beta''_{r''} x^{h''_{r''}} \end{aligned}$$

dargestellt werden mögen; wir denken sie uns nach fallenden Potenzen von x geordnet; die Zahlen β_i, β_i', β_i'' sind dann bis auf die Anordnung mit den Elementen α_i, α_i', α_i'' der Ideale $\mathfrak{a}, \mathfrak{a}', \mathfrak{a}''$ resp. identisch. Ist nun $\mathfrak{p}$ irgend ein Primideal des Körpers und $\mathfrak{p}^a, \mathfrak{p}^{a'}, \mathfrak{p}^{a''}$ die höchsten Potenzen desselben, durch welche die Ideale $\mathfrak{a}, \mathfrak{a}', \mathfrak{a}''$ teilbar sind, wobei die Exponenten a, a', a'' resp. gleich Null zu denken sind, falls $\mathfrak{p}$ gar kein Primidealfaktor des bezüglichen Ideals wäre, so sind alle Elemente β_i' zwar durch $\mathfrak{p}^{a'}$, wenigstens eins von ihnen aber nicht mehr durch $\mathfrak{p}^{a'+1}$ teilbar, da sonst gegen die Voraussetzung auch sämtliche Zahlen in $\mathfrak{a}'$ dies sein müßten; desgleichen werden alle Elemente β_i'' zwar durch $\mathfrak{p}^{a''}$, wenigstens eins derselben aber nicht mehr durch $\mathfrak{p}^{a''+1}$ teilbar sein. Man bezeichne mit β_k' das erste der Elemente $\beta_1', \beta_2', \cdots$, welches nicht mehr durch $\mathfrak{p}^{a'+1}$, mit β_k'' das erste der Elemente $\beta_1'', \beta_2'' \cdots$, welches nicht mehr durch $\mathfrak{p}^{a''+1}$ aufgeht. Dann erkennt man

ganz ähnlich wie bei dem Beweise des Gaußschen Fundamentalsatzes in Kap. 6, Nr. 3, daß dasjenige Glied

$$\beta_i x^{h_i}$$

der Funktion $F(x)$, dessen Exponent h_i gleich $h_k' + h_l''$ ist, einen Koeffizienten β_i haben muß, welcher zwar durch $\mathfrak{p}^{a'+a''}$, aber nicht mehr durch $\mathfrak{p}^{a'+a''+1}$ teilbar ist, während im übrigen gewiß sämtliche Koeffizienten dieser Funktion durch $\mathfrak{p}^{a'+a''}$ teilbar sind. Daher geht das Ideal

$$\{\beta_1, \beta_2, \cdots, \beta_r\},$$

welches mit dem Ideale $\mathfrak{a}$ identisch ist, genau durch $\mathfrak{p}^{a'+a'}$ auf. Jedes Primideal findet sich hiernach in der Zerlegung von $\mathfrak{a}$ genau so oft, wie in den Zerlegungen von $\mathfrak{a}'$, $\mathfrak{a}''$ zusammen genommen und folglich ist, wie der Satz es behauptet,

$$\mathfrak{a} = \mathfrak{a}' \cdot \mathfrak{a}''.$$

Das Ideal $\mathfrak{a}$ ist der größte gemeinsame Idealteiler der Hauptideale $\mathfrak{g}\alpha_1, \mathfrak{g}\alpha_2, \cdots, \mathfrak{g}\alpha_r$ oder der Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$; sind die letzteren ganze rationale Zahlen und δ deren größter gemeinsamer Teiler, so ist

$$\mathfrak{a} = \mathfrak{g}\delta,$$

da einerseits alle Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_r$, also auch das Ideal

$$\mathfrak{a} = \mathfrak{g}\alpha_1 + \mathfrak{g}\alpha_2 + \cdots + \mathfrak{g}\alpha_r$$

in $\mathfrak{g}\delta$, andererseits die Zahl δ, weil sie in die Form

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_r x_r$$

mit ganzen rationalen Werten der x_i gesetzt werden kann, und daher auch $\mathfrak{g}\delta$ in $\mathfrak{a}$ enthalten ist. In diesem Falle ist also der **Inhalt** der Form F im wesentlichen nichts anderes als das, was in Kap. 6, Nr. 3 der **Teiler** der Funktion F genannt worden ist, und so erhalten wir aus dem vorher bewiesenen fundamentalen Satze insbesondere den Satz, daß der Teiler eines Produkts ganzzahliger Funktionen gleich dem Produkte aus den Teilern der Funktionen ist, wieder zurück.

Aus dem fundamentalen Satze fließt sogleich weiter der Satz, daß, wenn ein Produkt von Formen durch ein Primideal $\mathfrak{p}$ teilbar ist, auch einer der Faktoren es sein muß. Denn, sind in (9) sämtliche Koeffizienten von F teilbar durch $\mathfrak{p}$, so geht $\mathfrak{a}$ und daher mindestens

dies der Fall, also die vorstehende Gleichung erfüllt ist, so folgt aus (14)

$$\{\beta_1, \beta_2, \cdots, \beta_s\} = \mathfrak{g}\mathsf{N},$$

mithin ist jede der Zahlen β_i teilbar durch N und Gleiches gilt demnach auch von den konjugierten Zahlen $\beta_i^{(1)}, \beta_i^{(2)}, \cdots, \beta_i^{(n-1)}$, also wird das Produkt der zu Φ konjugierten Funktionen:

$$\Phi^{(1)}\Phi^{(2)}\ldots\Phi^{(n-1)} = \frac{NF(u, v, \cdots)^{n-1}}{F^{(1)}F^{(2)}\ldots F^{(n-1)}} = F(u, v, \cdots)\cdot \mathsf{N}^{n-2}\cdot E(u, v, \cdots)^{n-2}$$

durch N^{n-1} teilbar sein, während der Inhalt der rechten Seite vorstehender Gleichung nur N^{n-2} ist; dies tritt nur ein, wenn $\mathsf{N} = 1$, und folglich ergibt sich $NF(u, v, \cdots)$ als eine primitive Form. — Aus diesem Satze ist zu ersehen, daß die Definition einer Einheitsform auch so gefaßt werden kann, zu sagen: Einheitsform heißt jede Form, deren Norm N gleich Eins ist.

Hieraus folgt dann weiter, daß zwei Formen von gleichem Inhalte voneinander nur um Faktoren verschieden sind, welche Einheitsformen sind, und daß umgekehrt zwei so voneinander verschiedene Formen gleichen Inhalt besitzen. In der Tat, besteht eine Gleichung

$$F_1 \cdot E = F \cdot E_1, \tag{15}$$

wo E, E_1 zwei Einheitsformen bedeuten, so ergibt sich, da dem Fundamentalsatze zufolge ihre beiden Seiten bezw. denselben Inhalt besitzen, wie F_1, F resp., unmittelbar, daß diese beiden Funktionen von gleichem Inhalte sind. Wenn aber umgekehrt F, F_1 zwei Formen gleichen Inhalts sind und Φ wie zuvor das aus den zu F konjugierten Funktionen gebildete Produkt bezeichnet, so haben dem Fundamentalsatze zufolge auch die Produkte $F\cdot\Phi$ und $F_1\cdot\Phi$ gleichen Inhalt, nämlich den Inhalt $\mathfrak{g}\mathsf{N}$ von NF, daher sind die Koeffizienten des letzten Produkts durch N teilbare ganze Zahlen des Körpers und

$$F_1\cdot\Phi = \mathsf{N}\cdot E_1,$$

wo E_1 eine Funktion bedeutet, deren Inhalt gleich $\mathfrak{g}$ ist. Die Verbindung dieser und der Gleichung (11) liefert aber die Gleichung (15), deren Bestehen behauptet war. Diesem Satze

gemäß darf man die Definition äquivalenter Formen auch durch die folgende ersetzen: Zwei Formen heißen äquivalent, wenn ihr Quotient gleich dem Quotienten zweier Einheitsformen ist.

Äquivalente Formen haben gleiche Norm, denn aus (15) folgt, da die Norm jeder Einheitsform gleich 1 ist, die Gleichung

$$\mathrm{N}_1 = \mathrm{N},$$

wenn N_1 analog mit N den Teiler von $N\mathrm{F}_1(u, v, \cdots)$ bedeutet.

5. Man kann nunmehr den Satz beweisen, daß die Norm einer Form stets gleich der Norm des Ideals ist, welches ihren Inhalt ausmacht. Der vorstehenden Bemerkung zufolge genügt es, dies für irgend eine Form mit dem Inhalte $\mathfrak{a}$ zu zeigen. Wir denken uns also das Ideal $\mathfrak{a}$ als Modulus:

$$\mathfrak{a} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$$

und wählen

$$\mathrm{F} = u_1\alpha_1 + u_2\alpha_2 + \cdots + u_n\alpha_n.$$

Sind dann $\gamma_1, \gamma_2, \cdots, \gamma_n$ die Basiszahlen von $\mathfrak{g}$, so werden die Produkte $\gamma_1\alpha_i, \gamma_2\alpha_i, \cdots, \gamma_n\alpha_i$ wieder Zahlen des Ideals $\mathfrak{a}$, mithin als lineare und homogene ganzzahlige Funktionen von $\alpha_1, \alpha_2, \cdots, \alpha_n$ darstellbar sein, und demnach werden n Gleichungen bestehen von der Form:

$$(16)\qquad \begin{aligned} \mathrm{F}\cdot\gamma_1 &= U_{11}\alpha_1 + U_{21}\alpha_2 + \cdots + U_{n1}\alpha_n \\ \mathrm{F}\cdot\gamma_2 &= U_{12}\alpha_1 + U_{22}\alpha_2 + \cdots + U_{n2}\alpha_n \\ &\cdots\cdots\cdots\cdots\cdots \\ \mathrm{F}\cdot\gamma_n &= U_{1n}\alpha_1 + U_{2n}\alpha_2 + \cdots + U_{nn}\alpha_n, \end{aligned}$$

in denen die Koeffizienten U_{ik} lineare ganzzahlige Funktionen der Unbestimmten u_i sind. Die Determinante

$$U = |U_{ik}|$$

wird also eine Form n^{ten} Grades mit diesen Unbestimmten sein, die, wie man leicht erkennt, eine Einheitsform ist. Wäre nämlich der größte gemeinsame Teiler ihrer Koeffizienten von 1 verschieden, also durch eine Primzahl p teilbar, so würden sich (vgl. Kap. 1, Nr. 7) ganze, ganzzahlige nicht sämtlich

durch p teilbare Formen $F_1, F_2, \cdots, F_n$ mit den Unbestimmten u_i angeben lassen von der Beschaffenheit, daß n Kongruenzen

$$U_{i1}F_1 + U_{i2}F_2 + \cdots + U_{in}F_n \equiv 0 \pmod{p}$$
$$(i = 1, 2, \cdots, n)$$

erfüllt wären, woraus dann hervorginge, daß der Ausdruck

$$\begin{aligned} &F(F_1\gamma_1 + F_2\gamma_2 + \cdots + F_n\gamma_n) \\ &= \sum_i (U_{i1}F_1 + U_{i2}F_2 + \cdots + U_{in}F_n)\,\alpha_i \end{aligned}$$

als eine Summe von Produkten, deren einer Faktor durch p teilbar, der andere eine Zahl des Ideals $\mathfrak{a}$ ist, lauter Koeffizienten hat, welche im Ideale $\mathfrak{g}p \cdot \mathfrak{a}$ enthalten sind. Der Inhalt desselben Ausdrucks ist aber $\mathfrak{a} \cdot \mathfrak{j}$, wenn $\mathfrak{j}$ denjenigen der Form

$$F_1\gamma_1 + F_2\gamma_2 + \cdots + F_n\gamma_n$$

bezeichnet; daher muß $\mathfrak{j}$, also jeder Koeffizient dieser Form, deren jeder die Gestalt einer linearen ganzzahligen Funktion

$$a_1\gamma_1 + a_2\gamma_2 + \cdots + a_n\gamma_n$$

hat, in $\mathfrak{g}p$ enthalten sein, was nur sein kann, wenn die sämtlichen a_i, nämlich alle Koeffizienten der Funktionen F_i durch p teilbar sind, gegen die Bedeutung der letzteren.

Nachdem dies für die Determinante U bewiesen ist, stelle man nun neben dem Systeme (16) die sämtlichen dazu konjugierten Systeme von Gleichungen auf; dann ergibt sich mittels des Multiplikationssatzes für Determinanten nachstehende Gleichung:

$$(17)\quad NF \cdot \begin{vmatrix} \gamma_1, & \gamma_2, & \cdots\cdots, & \gamma_n \\ \gamma_1^{(1)}, & \gamma_2^{(1)}, & \cdots\cdots, & \gamma_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_1^{(n-1)}, & \gamma_2^{(n-1)}, & \cdots, & \gamma_n^{(n-1)} \end{vmatrix} = U \cdot \begin{vmatrix} \alpha_1, & \alpha_2, & \cdots\cdots, & \alpha_n \\ \alpha_1^{(1)}, & \alpha_2^{(1)}, & \cdots\cdots, & \alpha_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_1^{(n-1)}, & \alpha_2^{(n-1)}, & \cdots, & \alpha_n^{(n-1)} \end{vmatrix}.$$

Nun bestehen aber zwischen der Basis des Ideals $\mathfrak{a}$ und der Basis von $\mathfrak{g}$ Gleichungen von der Gestalt

$$\alpha_i = c_{1i}\gamma_1 + c_{2i}\gamma_2 + \cdots + c_{ni}\gamma_n,$$
$$(i = 1, 2, \cdots, n)$$

deren Determinante (vgl. Kap. 4, (46)) gleich der Norm

$$\mathfrak{N}(\mathfrak{a}) = (\mathfrak{g}, \mathfrak{a})$$

des Ideals $\mathfrak{a}$ ist, und da hieraus die Gleichung

$$\begin{vmatrix} \alpha_1, & \alpha_2, & \cdots, & \alpha_n \\ \alpha_1^{(1)}, & \alpha_2^{(1)}, & \cdots, & \alpha_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_1^{(n-1)}, & \alpha_2^{(n-1)}, & \cdots, & \alpha_n^{(n-1)} \end{vmatrix} = |c_{ik}| \cdot \begin{vmatrix} \gamma_1, & \gamma_2, & \cdots, & \gamma_n \\ \gamma_1^{(1)}, & \gamma_2^{(1)}, & \cdots, & \gamma_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_1^{(n-1)}, & \gamma_2^{(n-1)}, & \cdots, & \gamma_n^{(n-1)} \end{vmatrix}$$

hervorgeht, liefert die Formel (17) diese andere:

$$N\mathrm{F} = \mathfrak{N}(\mathfrak{a}) \cdot U,$$

welche, da U als eine Einheitsform festgestellt worden ist, mit der behaupteten Gleichheit

$$\mathrm{N} = \mathfrak{N}(\mathfrak{a})$$

gleichbedeutend ist.

Die vorstehend entwickelten Betrachtungen verstatten, ein beliebiges Ideal des Körpers, das bisher stets nur als eine Gesamtheit von unendlich vielen Zahlen des letzteren aufgefaßt worden ist, durch einen geschlossenen algebraischen Ausdruck zu deuten oder darzustellen, indem man es durch eine beliebige der Formen ersetzt, deren Inhalt es ausmacht. Da Hensel in seinen Arbeiten sich dieser Kroneckerschen Anschauungsweise bedient, wollen auch wir bei der Darstellung derselben Gebrauch davon machen.

6. Unter einem individuellen Teiler der Diskriminante einer Zahl θ der Gattung $\mathfrak{G}$ haben wir jede Primzahl p verstanden, die im Index von θ, d. i. in der, in Formel (3) auftretenden Determinante

$$C = |c_{ik}|$$

aufgeht. Sie unterscheiden sich von den übrigen Primzahlen durch einen ferneren charakteristischen Umstand. Sei nämlich wieder

$$F(x) = 0 \tag{18}$$

die irreduktible ganzzahlige Gleichung n^{ten} Grades, durch welche θ bestimmt ist. Wenn dann zunächst p eine jener individuellen Primzahlen ist, so lassen sich (nach Kap. 1, Nr. 7) n ganze, nicht sämtlich durch p teilbare Zahlen $x_1, x_2, \cdots, x_n$ angeben von der Beschaffenheit, daß

$$c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n \equiv 0 \pmod{p}, \quad (i = 1, 2, \cdots, n) \tag{19}$$

also auch

$$x_1 + x_2\theta + \cdots + x_n\theta^{n-1} \equiv 0 \pmod{p} \tag{20}$$

wird, eine Kongruenz, welche lehrt, daß in diesem Falle $F(x) \equiv 0 \pmod{p}$ nicht die Kongruenz niedrigsten Grades ist, welcher (mod. p) die Zahl θ genügt. Ist dagegen p keine der individuellen Primzahlen, so kann θ keiner Kongruenz (mod. p) Genüge leisten, deren Grad geringer ist als der Grad n der Kongruenz $F(x) \equiv 0 \pmod{p}$, denn aus einer Kongruenz geringeren Grades, also von der Form (20) mit nicht lauter durch p teilbaren Koeffizienten ergäben sich durch Einsetzen der Werte (2) für $1, \theta, \theta^2, \cdots, \theta^{n-1}$ wegen der rationalen Unabhängigkeit der Zahlen γ_i die Kongruenzen (19), welche, da ihre Determinante durch p nicht aufgeht, die Teilbarkeit aller x_i durch p nach sich ziehen, also zu einem Widerspruch führen würden. Man darf hiernach sagen: Dann und nur dann ist die niedrigste ganzzahlige Kongruenz (mod. p), welcher die Zahl θ genügt, vom Grade n, wenn p kein individueller oder außerwesentlicher Teiler der Diskriminante von θ ist. Die bereits berührte Frage, ob eine Primzahl p im Index jeder Zahl θ der Gattung $\mathfrak{G}$ aufgeht oder nicht, oder ob sie, wie Kronecker es ausdrückt, gemeinsamer außerwesentlicher Teiler der Diskriminanten aller dieser Zahlen sei oder nicht, läuft demzufolge auf die andere hinaus: ob in bezug auf den Modulus p für jede jener Zahlen die niedrigste Kongruenz, der sie genügt, von geringerem Grade sei als n, oder nicht.

Man bedenke nun, daß alle ganzen Zahlen des Körpers erhalten werden, wenn man in der linearen Form

$$w_0 = \gamma_1 u_1 + \gamma_2 u_2 \cdots + \gamma_n u_n \tag{21}$$

den Unbestimmten u_i alle ganzzahligen Werte gibt. Daher heißt diese Form w_0 die Fundamentalform des Körpers. Nimmt man an Stelle der Basiszahlen γ_i ihre konjugierten Zahlen $\gamma_i^{(1)}, \gamma_i^{(2)}, \cdots, \gamma_i^{(n-1)}$, so entstehen $n-1$ zu w_0 konjugierte Formen, welche $w_0^{(1)}, w_0^{(2)}, \cdots, w_0^{(n-1)}$ heißen mögen; man bilde die Gleichung, deren Wurzeln diese n zu einander konjugierten Formen sind. Sie ist, wenn w eine Unbestimmte bezeichnet, die folgende:

$$(22) \qquad N(w - u_1\gamma_1 - u_2\gamma_2 - \cdots - u_n\gamma_n) = 0,$$

die darin auftretende Norm aber (nach Nr. 4) eine ganze, ganzzahlige Funktion der Unbestimmten $w, u_1, u_2, \cdots, u_n$ oder von der Form

$$w^n + U_1 w^{n-1} + U_2 w^{n-2} + \cdots + U_{n-1} w + U_n,$$

wo die U_i ganze, ganzzahlige Funktionen der Unbestimmten u_i bedeuten; indem wir diesen Ausdruck kurz

$$F(w;\, u_1, u_2, \cdots, u_n)$$

nennen, schreiben wir die Gleichung (22), wie folgt:

$$(23) \qquad F(w;\, u_1, u_2, \cdots, u_n) = 0.$$

Wie nun aus (21) sämtliche ganzen Zahlen des Körpers entstehen, indem man für die u_i alle rationalen ganzen Zahlen setzt, so entstehen auf gleiche Weise aus (23) die Gleichungen n^{ten} Grades, denen jene einzeln genügen. Statt also für alle diese besonderen Gleichungen zu untersuchen, ob sie in bezug auf eine gegebene Primzahl p als Modulus die Kongruenz niedrigsten Grades abgeben, der die bezügliche Zahl des Körpers genügt, liegt es nahe, die eine Gleichung (23), welche die Fundamentalform w_0 zur Wurzel hat und deshalb die Fundamentalgleichung des Körpers heißen soll, solcher Untersuchung zu unterwerfen. Wir stellen uns in der Tat zunächst die Frage, ob bezw. wann diese Gleichung, wenn man die Größen u_i unbestimmt läßt, (mod. p) irreduktibel sei, oder, was auf dasselbe hinauskommt, welches bei unbestimmt bleibenden u_i die Kongruenz geringsten Grades (mod. p) sei, der die Fundamentalform w_0 genügen kann.

Zu diesem Zwecke denken wir die Primzahl p in ihre Primidealfaktoren zerlegt:

$$(24) \qquad p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

wo allgemein $\mathfrak{p}_i$ ein Primideal und f_i sein Grad sei, sodaß dem Satze über die Norm eines Produkts zufolge und, da p^n die Norm von p ist, folgende Gleichung statt hat:

$$(25) \qquad n = e_1 f_1 + e_2 f_2 + \cdots + e_r f_r.$$

Wir betrachten eins jener Primideale $\mathfrak{p}$, nennen f seinen Grad

und stellen die vorige Frage zunächst in bezug auf den Modulus $\mathfrak{p}$ welches ist bei unbestimmt bleibenden u_i die niedrigste Kongruenz (mod. $\mathfrak{p}$), der w_0 genügt?

Zur Antwort sei

$$(26) \qquad \varphi(w;\, u_1,\, u_2,\, \cdots,\, u_n) \equiv 0 \pmod{\mathfrak{p}}$$

eine beliebige Kongruenz von derselben Art wie (23), welche w_0 zur Wurzel hat, d. h., wenn

$$\varphi(w;\, u_1,\, u_2,\, \cdots,\, u_n) = U_0' w^m + U_1' w^{m-1} + \cdots + U_m'$$

und die U_i' als ganze, ganzzahlige Funktionen der u_i gedacht werden, so sollen in der Form

$$U_0' w_0^m + U_1' w_0^{m-1} + \cdots + U_m'$$

mit den Unbestimmten u_i sämtliche Koeffizienten (der Inhalt der Form) durch das Primideal $\mathfrak{p}$ teilbar sein:

$$(27) \qquad \varphi(w_0;\, u_1,\, u_2,\, \cdots,\, u_n) \equiv 0 \pmod{\mathfrak{p}}.$$

Hieraus folgt durch Erhebung zur p^{ten} Potenz auch

$$\varphi(w_0;\, u_1,\, u_2,\, \cdots,\, u_n)^p \equiv 0 \pmod{\mathfrak{p}},$$

während dem polynomischen Satze zufolge diese p^{te} Potenz (mod. p), also auch (mod. $\mathfrak{p}$) mit dem Ausdrucke

$$\varphi(w_0^p;\, u_1^p,\, u_2^p,\, \cdots,\, u_n^p)$$

oder, da desgleichen

$$w_0^p \equiv u_1^p \gamma_1^p + u_2^p \gamma_2^p + \cdots + u_n^p \gamma_n^p \pmod{\mathfrak{p}}$$

ist, mit dem folgenden:

$$\varphi(u_1^p \gamma_1^p + \cdots + u_n^p \gamma_n^p;\, u_1^p,\, u_2^p,\, \cdots,\, u_n^p)$$

kongruent ist. Also ist auch dieser letztere kongruent Null, während die u_i unbestimmt bleiben; da dann aber die u_i^p ebensolche Unbestimmte bezeichnen, so darf man schließen, daß, wenn zur Abkürzung

$$(28) \qquad w_1 = \gamma_1^p u_1 + \gamma_2^p u_2 + \cdots + \gamma_n^p u_n$$

gesetzt wird,

$$\varphi(w_1;\, u_1,\, u_2,\, \cdots,\, u_n) \equiv 0 \pmod{\mathfrak{p}}$$

sei. Ist also w_0 eine Wurzel der Kongruenz (26), so ist's w_1

auch; und in gleicher Weise folgert man nun, daß, wenn allgemein

(29) $$w_k = \gamma_1^{p^k} u_1 + \gamma_2^{p^k} u_2 + \cdots + \gamma_n^{p^k} u_n$$

gesetzt wird, mit w_0 zugleich auch jede dieser Funktionen w_k eine Wurzel derselben Kongruenz sein muß.

Nun gibt es einen kleinsten Index k so beschaffen, daß bei unbestimmt bleibenden u_i

(30) $$w_k \equiv w_0 \pmod{\mathfrak{p}}$$

ist, und dieser Index k ist f. In der Tat ist diese Kongruenz gleichbedeutend mit dem Systeme der n Kongruenzen

(31) $$\gamma_i^{p^k} \equiv \gamma_i \pmod{\mathfrak{p}}, \quad (i = 1, 2, \cdots, n)$$

welche für $k = f$ dem Fermatschen Satze zufolge erfüllt sind, mithin ist $w_f \equiv w_0 \pmod{\mathfrak{p}}$. Bestünden die Kongruenzen (31) aber schon für einen kleineren Wert von k, so würde, da jede ganze Zahl γ des Körpers von der Gestalt

$$\gamma = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_n\gamma_n$$

ist, aus welcher

$$\gamma^{p^k} \equiv a_1\gamma_1^{p^k} + a_2\gamma_2^{p^k} + \cdots + a_n\gamma_n^{p^k} \pmod{\mathfrak{p}}$$

hervorgeht, jede solche Zahl die Kongruenz

$$\gamma^{p^k} \equiv \gamma \pmod{\mathfrak{p}} \quad (k < f)$$

erfüllen, während es Zahlen gibt, welche (mod. $\mathfrak{p}$) zum Exponenten f passen. — Von den f Funktionen $w_0, w_1, \cdots, w_{f-1}$ aber überzeugt man sich leicht, daß sie (mod. $\mathfrak{p}$) inkongruent sind. Denn aus einer Kongruenz

$$w_{g+k} \equiv w_g \pmod{\mathfrak{p}},$$

in welcher g und $g + k$ Zahlen der Reihe $0, 1, 2, \cdots, f-1$ bedeuten, ergäben sich die n Kongruenzen

$$\gamma_i^{p^{g+k}} \equiv \gamma_i^{p^g}, \quad (i = 1, 2, \cdots, n)$$

welche zur Potenz p^{f-g} erhoben die anderen:

$$\gamma_i^{p^{f+k}} \equiv \gamma_i^{p^f}$$

d. i. mit Rücksicht auf den Fermatschen Satz diese neuen:

$$\gamma_i^{p^k} \equiv \gamma_i \quad (k < f)$$
$$(i = 1, 2, \cdots, n)$$

nach sich ziehen würden, die, wie soeben gezeigt worden, nicht stattfinden können.

Aus all' diesem ist also der Schluß zu ziehen, daß die Kongruenz (26), sobald sie die Wurzel w_0 hat, stets die f inkongruenten Wurzeln

$$w_0, \; w_1, \; w_2, \; \cdots, \; w_{f-1}$$

besitzt.

Zugleich ist aber dann die Funktion $\varphi(w; u_1, u_2, \cdots, u_n)$ (mod. $\mathfrak{p}$) teilbar durch $w - w_0$, d. h. es besteht eine Kongruenz

$$\varphi(w) \equiv (w - w_0) \cdot \varphi_1(w) \quad (\text{mod. } \mathfrak{p}),$$

in welcher $\varphi_1(w)$, wie $\varphi(w)$, eine ganze Funktion von w und den u_i mit algebraisch ganzzahligen Koeffizienten bedeutet. Da nun $\varphi(w_1) \equiv 0$ ist, muß auch

$$(w_1 - w_0) \cdot \varphi_1(w_1) \equiv 0 \quad (\text{mod. } \mathfrak{p})$$

sein, mithin, da der erste Faktor dieses Produkts ganzer Funktionen der u_i nicht teilbar ist durch $\mathfrak{p}$, muß nach Nr. 3

$$\varphi_1(w_1) \equiv 0 \quad (\text{mod. } \mathfrak{p})$$

sein, woraus dann wieder $\varphi_1(w)$ durch $w - w_1$ (mod. $\mathfrak{p}$) teilbar hervorgeht, usw., sodaß sich schließlich

$$\varphi(w) \equiv f(w) \cdot \psi(w) \quad (\text{mod. } \mathfrak{p}) \tag{32}$$

ergibt, worin

$$f(w) = (w - w_0)(w - w_1) \cdots (w - w_{f-1}) \tag{33}$$

gesetzt und $\psi(w)$ eine ganze Funktion von w und den u_i mit algebraisch ganzzahligen Koeffizienten ist. Die Koeffizienten der Funktion $f(w)$ sind, wie sich unschwer nachweisen läßt, rationalen ganzen Zahlen (mod. $\mathfrak{p}$) kongruent. In der Tat folgt aus (33)

$$f(w)^p \equiv (w^p - w_0^p)(w^p - w_1^p) \cdots (w^p - w_{f-1}^p) \quad (\text{mod. } \mathfrak{p}); \tag{34}$$

nun ist aber nach (29)

$$w_k^p \equiv \gamma_1^{p^{k+1}} u_1^p + \gamma_2^{p^{k+1}} u_2^p + \cdots + \gamma_n^{p^{k+1}} u_n^p,$$

ein Ausdruck, der sich aus den γ_i und den u_i^p genau so zusammensetzt, wie w_{k+1} aus den γ_i und den u_i; demnach entsteht der Ausdruck zur Rechten von (34) aus dem Ausdrucke

$$(w^p - w_1)(w^p - w_2) \cdots (w^p - w_f)$$

oder dem ihm (mod. $\mathfrak{p}$) kongruenten Ausdrucke

$$(w^p - w_0)(w^p - w_1) \cdots (w^p - w_{f-1})$$

einfach dadurch, daß man die u_i durch die u_i^p ersetzt; und so erkennt man die Richtigkeit folgender Formel:

$$f(w;\, u_1,\, u_2,\, \cdots,\, u_n)^p \equiv f(w^p;\, u_1^p,\, u_2^p,\, \cdots,\, u_n^p) \quad (\text{mod. } \mathfrak{p}).$$

Versteht man aber unter

$$\alpha w^s \cdot u_1^{h_1} u_2^{h_2} \cdots u_n^{h_n}$$

irgend ein Glied der Funktion $f(w; u_1, u_2, \cdots, u_n)$, so reduziert sich die linke Seite der vorigen Kongruenz (mod. $\mathfrak{p}$) auf die Summe der Glieder

$$\alpha^p w^{ps} \cdot u_1^{h_1 p} u_2^{h_2 p} \ldots u_n^{h_n p},$$

und zur Rechten steht die Summe der Glieder

$$\alpha w^{ps} \cdot u_1^{h_1 p} u_2^{h_2 p} \cdots u_n^{h_n p},$$

also erfüllen die sämtlichen dem Körper angehörigen Koeffizienten α der Funktion $f(w)$ die Kongruenz

$$\alpha^p \equiv \alpha \quad (\text{mod. } \mathfrak{p})$$

und sind demnach (vgl. vor. Kap., Nr. 21), wie behauptet, rationalen ganzen Zahlen (mod. $\mathfrak{p}$) kongruent. Nennt man $\mathfrak{F}(w)$ die ganze, ganzzahlige Funktion von w und den u_i, welche (mod. $\mathfrak{p}$) kongruent $f(w)$ ist, und durch welche also wegen (32) die Funktion $\varphi(w)$ (mod. $\mathfrak{p}$) teilbar ist, so entsteht eine Kongruenz von der Form

$$\varphi(w) \equiv \mathfrak{F}(w) \cdot \chi(w) \quad (\text{mod. } \mathfrak{p}), \tag{35}$$

in welcher nun, da der höchste Koeffizient von $\mathfrak{F}(w)$ die Eins ist, zugleich mit $\varphi(w)$ auch die Funktion $\chi(w)$ r a t i o n a l e ganze Koeffizienten haben muß. Rationale ganze Zahlen, welche

(mod. $\mathfrak{p}$) kongruent sind, deren Differenz also in $\mathfrak{p}$ enthalten und daher als rationale ganze Zahl durch p teilbar ist, sind einander auch (mod. p) kongruent; sonach besteht die voraufgehende Kongruenz auch (mod. p):

$$(36) \qquad \varphi(w) \equiv \mathfrak{F}(w) \cdot \chi(w) \pmod{p}.$$

So oft also $\varphi(w)$ die Fundamentalform w_0 (mod. $\mathfrak{p}$) zur Wurzel hat, ist die Funktion $\varphi(w)$ bei unbestimmt bleibenden u_i (mod. p) teilbar durch die Funktion $\mathfrak{F}(w)$, und selbstverständlich gilt das Umgekehrte auch.

Hieraus aber schließt man weiter, daß die Kongruenz

$$(37) \qquad \mathfrak{F}(w) \equiv 0 \pmod{\mathfrak{p}},$$

deren Grad derjenige des Primideals $\mathfrak{p}$ ist, die Kongruenz niedrigsten Grades ist, welcher (mod. $\mathfrak{p}$) die Fundamentalform w_0 genügt.

Die Funktion $\mathfrak{F}(w)$ muß daher bei unbestimmt bleibenden u_i (mod. p) auch irreduktibel sein. Denn, bestände eine Kongruenz von der Form

$$\mathfrak{F}(w) \equiv F_1(w) \cdot F_2(w) \pmod{p},$$

so bestände sie umsomehr auch (mod. $\mathfrak{p}$), und da w_0 die linke Seite durch $\mathfrak{p}$ teilbar macht, so müßte (vgl. Nr. 3) auch eine der Kongruenzen

$$F_1(w) \equiv 0, \; F_2(w) \equiv 0 \pmod{\mathfrak{p}}$$

geringeren als f^{ten} Grades durch die Fundamentalform befriedigt werden, dem eben bewiesenen Satze zuwider.

Man darf dem erhaltenen Resultate den Ausspruch hinzufügen, daß das Ideal $\mathfrak{p}$ der Inhalt der Form

$$pz + \mathfrak{F}(w_0)$$

sei und daher in *Kronecker*scher Weise durch dieselbe ausdrückbar sei, in Zeichen:

$$(38) \qquad \mathfrak{p} \sim pz + \mathfrak{F}(w_0).$$

In der Tat: jeder Idealteiler der Koeffizienten dieses Ausdrucks würde auch ein Teiler desselben bleiben, wenn die Unbestimmten u_i durch irgend welche rationale ganze Zahlen

ersetzt würden, wodurch w_0 in irgend eine ganze Zahl des Körpers überginge. Denkt man sich dies so getan, daß w_0 in die im vorigen Kapitel, Nr. 22 mit ϱ bezeichnete Zahl übergeht, für welche

$$(39) \qquad \mathfrak{p} = \{p,\ P(\varrho)\}$$

ist, und bemerkt, daß gleichzeitig $\mathfrak{F}(w)$ in eine ganze, ganzzahlige Funktion f^{ten} Grades übergeht, welcher der Wert ϱ von w_0 (mod. $\mathfrak{p}$) Genüge tut, und welche somit keine andere sein kann, als die (mod. $\mathfrak{p}$) irreduktible Funktion $P(w)$, so sieht man, daß $\mathfrak{F}(w_0)$ in $P(\varrho)$ übergeht, mithin jener Idealteiler der Form (38) ein gemeinsamer Teiler von p und $P(\varrho)$ sein muß. Da nun offenbar der größte gemeinsame Teiler $\mathfrak{p}$ dieser Zahlen in der Form (38) aufgeht, so muß $\mathfrak{p}$, wie behauptet, der Inhalt derselben sein.

7. Nachdem dies festgestellt worden, denke man sich einen zweiten, dem Idealteiler $\mathfrak{p}$ gleichen oder davon verschiedenen Primidealteiler $\mathfrak{p}'$ von p und nenne f' seinen Grad; ihm entspricht analog der Kongruenz (37) eine ganze, ganzzahlige (mod. p) irreduktible Kongruenz niedrigsten, nämlich f'^{ten} Grades

$$\mathfrak{F}'(w) \equiv 0 \quad (\text{mod. } \mathfrak{p}'),$$

welcher die Fundamentalform w_0 genügt. Geht nun $\mathfrak{p}\mathfrak{p}'$ in p auf, so gilt der neue Satz: So oft die Kongruenz

$$(40) \qquad \varphi(w) \equiv 0 \quad (\text{mod. } \mathfrak{p}\mathfrak{p}')$$

die Fundamentalform w_0 zur Wurzel hat, ist die Funktion $\varphi(w)$ bei unbestimmt bleibenden u_i teilbar durch das Produkt $\mathfrak{F}(w) \cdot \mathfrak{F}'(w)$ (mod. p), und umgekehrt. Die Kongruenz niedrigsten Grades also, der w_0 (mod. $\mathfrak{p}\mathfrak{p}'$) genügt, ist die Kongruenz

$$(41) \qquad \mathfrak{F}(w) \cdot \mathfrak{F}'(w) \equiv 0 \quad (\text{mod. } \mathfrak{p}\mathfrak{p}').$$

Um dies einzusehen, bemerke man, daß, damit w_0 die Kongruenz (40) erfülle, woraus

$$\varphi(w_0) \equiv 0 \quad (\text{mod. } \mathfrak{p})$$

folgt, dem Satze der vorigen Nummer zufolge die Kongruenz

$$\varphi(w) \equiv \mathfrak{F}(w) \cdot \chi(w) \quad (\text{mod. } p)$$

notwendig und hinreichend ist. Da aus der letztern aber die Kongruenz

$$\varphi(w_0) \equiv \mathfrak{F}(w_0) \cdot \chi(w_0) \equiv 0 \pmod{\mathfrak{p}\mathfrak{p}'}$$

hervorgeht und man dieser die Form geben kann:

$$\frac{\mathfrak{F}(w_0)}{\mathfrak{p}} \cdot \chi(w_0) \equiv 0 \pmod{\mathfrak{p}'},$$

in welcher der erste Faktor keinen Primfaktor von p hat, da $\mathfrak{p}$ größter gemeinsamer Teiler von p und $\mathfrak{F}(w_0)$ ist, so muß der zweite Faktor $\chi(w_0)$ durch $\mathfrak{p}'$ teilbar sein, für welchen Umstand nach voriger Nummer eine Kongruenz von der Gestalt

$$\chi(w) \equiv \mathfrak{F}'(w) \cdot \psi(w) \pmod{p}$$

notwendig und hinreichend ist. Somit ergibt sich die Kongruenz

$$\varphi(w) \equiv \mathfrak{F}(w)\, \mathfrak{F}'(w) \cdot \psi(w) \pmod{p}$$

als die adäquate Bedingung für das Stattfinden der Kongruenz

$$\varphi(w_0) \equiv 0 \pmod{\mathfrak{p}\mathfrak{p}'},$$

wie behauptet, und hieraus fließt die weitere, im letzten Satze ausgesprochene Folgerung von selbst.

Die Ausdehnung dieser Betrachtung von zwei auf beliebig viel Primidealteiler von p führt schließlich zu folgendem Endergebnisse: Man denke sich für die verschiedenen Primidealteiler $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ von p die mit $\mathfrak{F}(w)$ analogen ganzen und ganzzahligen, (mod. p) irreduktibeln Funktionen

$$\mathfrak{F}_1(w), \; \mathfrak{F}_2(w), \; \cdots, \; \mathfrak{F}_r(w)$$

resp. von den Graden $f_1, f_2, \cdots, f_r$ bestimmt. Diese Funktionen sind von einander verschieden; denn, wären z. B. $\mathfrak{F}_1(w)$, $\mathfrak{F}_2(w)$ ein- und dieselbe Funktion, so folgte daraus wegen

$$\mathfrak{p}_1 \sim pz + \mathfrak{F}_1(w_0), \; \mathfrak{p}_2 \sim pz + \mathfrak{F}_2(w_0)$$

die Gleichheit von $\mathfrak{p}_1, \mathfrak{p}_2$ gegen die Voraussetzung. Damit eine Kongruenz

$$\varphi(w) \equiv 0 \pmod{p} \tag{42}$$

die Fundamentalform w_0 zur Wurzel hat, ist die adäquate Bedingung, daß eine Kongruenz statthabe von der Form

$$(43) \quad \varphi(w) \equiv \mathfrak{F}_1(w)^{e_1} \cdot \mathfrak{F}_2(w)^{e_2} \cdots \mathfrak{F}_r(w)^{e_r} \cdot \psi(w) \pmod{p},$$

in welcher $\psi(w)$ eine ganze, ganzzahlige Funktion von w und den u_i bedeutet. Die Kongruenz niedrigsten Grades (mod. p), welcher die Fundamentalform genügt, ist also die Kongruenz

$$(44) \quad \mathfrak{F}_1(w)^{e_1} \cdot \mathfrak{F}_2(w)^{e_2} \cdots \mathfrak{F}_r(w)^{e_r} \equiv 0 \pmod{p},$$

deren Grad mit Beachtung der Gleichung (25) sich gleich n, nämlich gleich dem Grade der Fundamentalgleichung ergibt. Für keine Primzahl p kann demnach die Fundamentalform w_0 eine Kongruenz geringeren Grades als der der Fundamentalgleichung erfüllen. Da aber die Fundamentalgleichung für $w = w_0$ erfüllt wird, so gilt dasselbe auch für die Kongruenz

$$F(w) \equiv 0 \pmod{p},$$

und folglich muß wegen (43)

$$F(w) \equiv \mathfrak{F}_1(w)^{e_1} \mathfrak{F}_2(w)^{e_2} \cdots \mathfrak{F}_r(w)^{e_r} \cdot \psi(w) \pmod{p},$$

oder vielmehr, da F denselben Grad und denselben höchsten Koeffizienten 1 hat, wie das Produkt in (44), so muß genauer

$$(45) \quad F(w) \equiv \mathfrak{F}_1(w)^{e_1} \cdot \mathfrak{F}_2(w)^{e_2} \cdots \mathfrak{F}_r(w)^{e_r} \pmod{p}$$

sein. Die Funktionen $\mathfrak{F}_i(w)$ sind aber irreduktibel oder Primfunktionen (mod. p), und somit stellt die vorstehende Formel die nur auf eine Weise mögliche Zerlegung der Funktion $F(w)$ der Fundamentalgleichung in ein Produkt von Primfunktionen (mod. p) dar.

Von diesem wichtigen Resultate, welches mit einer gewissen Beschränkung schon von Kronecker (Festschrift § 25), in seiner ganzen Vollständigkeit aber zuerst von Hensel a. a. O. begründet worden ist, wieder zurückschließend erkennt man nun, wie im Gegensatze zu dem in Nr. 1 Bemerkten bei Einführung der Unbestimmten u_i für jede Primzahl p ohne Ausnahme die Theorie der höheren Kongruenzen (mod. p) zur Zerlegung von p in seine Primidealfaktoren und zur Aufstellung dieser benutzt werden kann. In der Tat braucht man offenbar nur mittels jener Theorie (vgl. Nr. 2) die ganze, ganzzahlige Funktion $F(w)$ von w und den u_i, welche die linke Seite der Fundamentalgleichung bildet, in ihre Primfaktoren (mod. p) zu zerlegen; ergibt sich dafür

die Zerlegung (45), worin die (mod. p) irreduktibeln Funktionen $\mathfrak{F}_i(w)$ bez. von den Graden f_i sind, so ergibt sich für die Primzahl p ihre Zerlegung in Primidealfaktoren nach folgender Formel:

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}, \tag{46}$$

wo allgemein das Primideal $\mathfrak{p}_i$ vom Grade f_i und durch die Formel

$$\mathfrak{p}_i \sim pz + \mathfrak{F}_i(w_0) \tag{47}$$

bestimmt ist.

Hieran schließt sich ein Satz, der gleichfalls mit der erwähnten Beschränkung schon von Kronecker ausgesprochen, doch erst von Hensel auf Grund der vorigen Resultate voll bewiesen worden ist. Aus der Formel

$$w_0 = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_n u_n$$

der Fundamentalform ergeben sich, analog den Gleichungen (2) die n Beziehungen

$$w_0^i = U_{1i}\gamma_1 + U_{2i}\gamma_2 + \cdots + U_{ni}\gamma_n, \quad (i = 0, 1, 2, \cdots, n-1) \tag{48}$$

in denen die Koeffizienten U_{ik} ganze, ganzzahlige Funktionen der Unbestimmten u_i bezeichnen, und aus ihnen die der Gleichung (3) entsprechende Formel:

$$\Delta(1, w_0, w_0^2, \cdots, w_0^{n-1}) = U^2 \cdot \Delta(\mathfrak{g}), \tag{49}$$

in welcher

$$U = |U_{ik}| \tag{50}$$

gleichfalls eine ganze, ganzzahlige Funktion der u_i ist; als solche soll sie bezeichnet werden durch

$$U = \vartheta(u_1, u_2, \cdots, u_n), \tag{51}$$

wodurch die Gleichung (49) übergeht in die folgende:

$$\Delta(1, w_0, w_0^2, \cdots, w_0^{n-1}) = \Delta(\mathfrak{g}) \cdot \vartheta(u_1, u_2, \ldots, u_n)^2. \tag{52}$$

Es wird behauptet, daß die Funktion (51), mithin auch ihr Quadrat eine Einheitsform ist. Wäre sie nämlich, d. i. die Determinante der Gleichungen (48), durch irgend eine Primzahl p teilbar, so gäbe es (nach Kap. 1, Nr. 7) n ganze und ganzzahlige Funktionen $U_1, U_2, \cdots, U_n$ der U_{ik},

also auch der u_i, die nicht sämtlich durch p teilbar und so beschaffen sind, daß die Kongruenzen

$$U_{i1} U_1 + U_{i2} U_2 + \cdots + U_{in} U_n \equiv 0 \pmod{p}$$
$$(i = 0, 1, 2, \cdots, n-1)$$

stattfinden, woraus dann die folgende:

$$U_1 + U_2 w_0 + U_3 w_0^2 + \cdots + U_n w_0^{n-1} \equiv 0 \pmod{p}$$

hervorginge, welche doch mit dem allgemeinen, zuvor bewiesenen Satze unverträglich ist. Aus dieser Erkenntnis folgt aber sogleich nach Formel (52) der Satz:

Die Diskriminante der Fundamentalgleichung:

$$(53) \qquad \Delta(1, w_0, w_0^2, \cdots, w_0^{n-1})$$

ist (im *Kronecker*schen Sinne) der Diskriminante oder der Grundzahl des Körpers äquivalent, oder, was dasselbe sagt, ihr Teiler bei unbestimmt bleibenden u_i ist die Grundzahl des Körpers.

8. Diese bei Beibehaltung der u_i als unbestimmter Größen für jede Primzahl p ohne Ausnahme geltenden Verhältnisse komplizieren sich nun sogleich, wenn man von der Fundamentalform w_0 zu bestimmten Zahlen θ des Körpers übergeht, wegen der Scheidung der Primzahlen in wesentliche und außerwesentliche Teiler der Diskriminante von θ. Setzt man für die Unbestimmten u_i bestimmte ganze Zahlen a_i, wodurch w_0 übergehe in eine Zahl θ der Gattung $\mathfrak{G}$, so verwandelt sich die Formel (52) in die folgende:

$$(54) \qquad \Delta(1, \theta, \theta^2, \cdots, \theta^{n-1}) = \Delta(\mathfrak{g}) \cdot \vartheta(a_1, a_2, \cdots, a_n)^2$$

und lehrt, daß die ganze rationale Zahl $\vartheta(a_1, a_2, \cdots, a_n)$ mit dem sogenannten Index von θ identisch ist. Zugleich gehen die Funktionen $\mathrm{F}(w)$ und $\mathfrak{F}_i(w)$ über in gewisse ganze, ganzzahlige Funktionen von w von demselben Grade wie jene, die wir $F(w)$, $P_i(w)$ resp. nennen wollen, sodaß aus der Kongruenz (45), wenn man die Variable w lieber durch das Zeichen x ersetzt, sich die folgende:

$$(55) \qquad F(x) \equiv P_1(x)^{e_1} P_2(x)^{e_2} \cdots P_r(x)^{e_r} \pmod{p}$$

ergibt, wobei

$$(56) \qquad F(x) = 0$$

die Gleichung bezeichnet, durch welche die Zahl θ bestimmt

ist. Die in der Zahl $\vartheta(a_1, a_2, \cdots, a_n)$ aufgehenden Primzahlen p sind die individuellen oder außerwesentlichen Teiler der Diskriminante von θ. Daher kommt die Frage, ob es gemeinsame außerwesentliche Teiler gibt, Primzahlen nämlich, die im Index jeder Zahl θ aufgehen, auf die andere Frage hinaus, ob die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ für alle ganzzahligen Wertsysteme der Unbestimmten u_i durch ein- und dieselbe Primzahl p teilbar sei oder nicht.

Diese Frage aber ist nach Nr. 8 des dritten Kapitels sogleich zu beantworten, und so erhält man folgenden Satz:

Damit eine Primzahl p gemeinsamer außerwesentlicher Teiler der Diskriminanten aller Zahlen der Gattung $\mathfrak{G}$ sei, ist notwendig und hinreichend, daß die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ in dem Modulus

$$\{p, u_1^p - u_1, u_2^p - u_2, \cdots, u_n^p - u_n\}$$

enthalten, nämlich von der Form:

$$\vartheta(u_1, u_2, \cdots, u_n) = p \cdot U + (u_1^p - u_1) \cdot U_1 + \cdots + (u_n^p - u_n) \cdot U_n$$

sei, in welcher $U, U_1, U_2, \cdots, U_n$ ganze, ganzzahlige Funktionen der u_i bezeichnen. Auch dieser Satz ist in der angegebenen präcisen Fassung Hensel zu verdanken.

Andererseits wissen wir aus Nr. 6, daß dann und nur dann die Kongruenz geringsten Grades

$$\varphi(x) \equiv 0 \pmod{p}, \tag{57}$$

welcher θ genügt, vom n^{ten} Grade ist, wenn p kein Teiler des Index von θ ist.

Untersucht man nun, welche Beschaffenheit der Funktionen $P_i(x)$ hierfür erforderlich sei, so erkennt man einfach, daß sie verschiedene Primfunktionen (mod. p) sein müssen. Wäre nämlich erstens eine dieser Funktionen, etwa $P_1(x)$, (mod. p) reduktibel, sodaß eine Kongruenz bestände von der Form

$$P_1(x) \equiv F_1(x) \cdot F_2(x) \pmod{p}, \tag{58}$$

so bestände diese auch (mod. $\mathfrak{p}_1$). Da nun bei unbestimmt bleibenden u_i die Funktion $\mathfrak{F}_1(w_0)$ durch $\mathfrak{p}_1$ teilbar ist, so wird sie es auch bleiben, wenn sie durch die Substitution der be-

stimmten Zahlen a_i an Stelle der u_i in $P_1(\theta)$ übergeht, und somit folgert man aus der Kongruenz (58) diese andere:

$$0 \equiv F_1(\theta) \cdot F_2(\theta) \pmod{\mathfrak{p}_1},$$

aus welcher wieder folgt, daß einer der Faktoren, etwa $F_1(\theta)$, durch $\mathfrak{p}_1$ aufgeht. Dann wäre aber bereits

$$F_1(\theta)^{e_1} \cdot P_2(\theta)^{e_2} \cdots P_r(\theta)^{e_r}$$

teilbar durch p, d. h. θ eine Wurzel der Kongruenz

$$F_1(x)^{e_1} \cdot P_2(x)^{e_2} \cdots P_r(x)^{e_r} \equiv 0 \pmod{p},$$

deren Grad geringer ist als n. — Wären zweitens zwei der Funktionen $P_i(x)$ zwar Primfunktionen, aber nicht verschieden, d. h. inkongruent (mod. p), sondern wäre z. B. $P_1(x) \equiv P_2(x)$ (mod. p), so sei etwa $e_1 \gtreqless e_2$. Da vorstehende Kongruenz auch nach jedem der beiden Moduln $\mathfrak{p}_1$, $\mathfrak{p}_2$ erfüllt sein muß und

$$P_1(\theta) \equiv 0 \pmod{\mathfrak{p}_1}, \quad P_2(\theta) \equiv 0 \pmod{\mathfrak{p}_2}$$

ist, so folgt notwendig auch $P_1(\theta) \equiv 0$ (mod. $\mathfrak{p}_2$); demnach wäre $P_1(\theta)^{e_1}$ sowohl durch $\mathfrak{p}_1^{e_1}$ als durch $\mathfrak{p}_2^{e_2}$ und somit

$$P_1(\theta)^{e_1} \cdot P_3(\theta)^{e_3} \cdots P_r(\theta)^{e_r}$$

durch p teilbar, mithin θ bereits eine Wurzel der Kongruenz

$$P_1(x)^{e_1} \cdot P_3(x)^{e_3} \cdots P_r(x)^{e_r} \equiv 0 \pmod{p},$$

deren Grad geringer ist als n. — Hieraus schließt man zunächst, daß zur Existenz einer Zahl, in deren Index die Primzahl

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$$

nicht enthalten sei, das Vorhandensein von r inkongruenten Primfunktionen (mod. p), deren Grade denjenigen der Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ gleich sind, erforderlich ist.

Man darf aber hinzufügen, daß diese für die Existenz einer solchen Zahl notwendige Bedingung auch die dafür ausreichende ist. Um dies zu beweisen, wähle man für jedes der Primideale $\mathfrak{p}_i$ nach Nr. 22 vorigen Kapitels eine beliebige Primfunktion $P_i(x)$ (mod. p), deren Grad f_i demjenigen des Primideals $\mathfrak{p}_i$ gleich ist, wie es eine solche nach Kap. 3, Nr. 5 stets gibt, und denke diejenige Wurzel ϱ_i der Kongruenz

(59) $$P_i(x) \equiv 0 \pmod{\mathfrak{p}_i}$$

bestimmt, für welche die Gleichheit

$$\mathfrak{p}_i = \{p,\ P_i(\varrho_i)\}$$

erfüllt ist, wo nämlich $P_i(\varrho_i)$ zwar durch $\mathfrak{p}_i$ aber nicht mehr durch $\mathfrak{p}_i^2$ teilbar ist. Bestimmt man alsdann, was möglich ist, eine Zahl ϱ den Kongruenzen

$$\varrho \equiv \varrho_i \ (\text{mod. } \mathfrak{p}_i^2)$$
$$(i = 1, 2, \cdots, r)$$

gemäß, so folgen daraus die anderen:

$$P_i(\varrho) \equiv P_i(\varrho_i) \ (\text{mod. } \mathfrak{p}_i^2),$$
$$(i = 1, 2, \cdots, r)$$

sodaß die Zahl $P_i(\varrho)$ je das zugehörige Primideal $\mathfrak{p}_i$ einmal, aber auch nur einmal als Faktor enthält. Nun sieht man leicht ein, daß eine Kongruenz

$$\varphi(\varrho) \equiv 0 \ (\text{mod. } \mathfrak{p}_i^{e_i}), \tag{60}$$

deren Koeffizienten rationale, nicht sämtlich durch p teilbare ganze Zahlen sind, völlig gleichbedeutend ist mit der folgenden:

$$\varphi(x) \equiv 0 \ \text{mod. } \{p,\ P_i(x)^{e_i}\}. \tag{61}$$

In der Tat, falls diese erfüllt ist, nämlich

$$\varphi(x) \equiv P_i(x)^{e_i} \cdot \psi(x) \ (\text{mod. } p)$$

gesetzt werden kann, so ergibt sich daraus für $x = \varrho$, da $P_i(\varrho)^{e_i}$ und p durch $\mathfrak{p}_i^{e_i}$ teilbar sind, auch die Kongruenz (60). Ist aber die Kongruenz (61) nicht erfüllt, d. h. $\varphi(x)$ (mod. p) nicht durch $P_i(x)^{e_i}$ teilbar, so muß der größte (mod. p) gemeinsame Teiler von $\varphi(x)$ und $P_i(x)^{e_i}$ gewiß eine Potenz $P_i(x)^h$ sein, wo $h < e_i$; daher besteht, unter $F_1(x)$, $F_2(x)$ ganze, ganzzahlige Funktionen verstanden, eine Kongruenz von der Gestalt

$$\varphi(x) \cdot F_1(x) + P_i(x)^{e_i} \cdot F_2(x) \equiv P_i(x)^h \ (\text{mod. } p),$$

aus welcher für $x = \varrho$ sich die andere

$$\varphi(\varrho) \cdot F_1(\varrho) \equiv P_i(\varrho)^h \ (\text{mod. } \mathfrak{p}_i^{e_i})$$

ergibt, welche lehrt, daß $\varphi(\varrho)$ nicht durch $\mathfrak{p}_i^{e_i}$ teilbar sein kann, da $P_i(\varrho)^h$ nur die Potenz $\mathfrak{p}_i^h < \mathfrak{p}_i^{e_i}$ zum Teiler hat.

Auf Grund dieser Bemerkung leuchtet ein, daß die Kongruenz

$$\varphi(\varrho) \equiv 0 \ (\text{mod. } p), \tag{62}$$

weil gleichbedeutend mit dem Systeme der Kongruenzen

von der Gestalt (60) für $i = 1, 2, \cdots, r$, auch gleichbedeutend mit dem Systeme nachstehender Kongruenzen:

$$(63) \qquad \varphi(x) \equiv 0 \text{ mod. } \{p, P_i(x)^{e_i}\} \quad (i = 1, 2, \cdots, r)$$

sein muß.

Hierbei waren bisher die Funktionen $P_i(x)$ ganz beliebige der Primfunktionen (mod. p) von den bezüglichen Graden f_i, wie sie immer vorhanden sind. Gibt es nun aber, wie in dem zu erhärtenden Ausspruche vorausgesetzt wird, r (mod. p) inkongruente Primfunktionen $P_i(x)$ dieser bezüglichen Grade, und setzt man, im vorigen diese für $P_i(x)$ wählend,

$$R(x) = P_1(x)^{e_1} \cdot P_2(x)^{e_2} \cdots P_r(x)^{e_r},$$

ein Ausdruck, dessen Grad wegen (25) gleich n ist, so ist wieder das System der r Kongruenzen (63) völlig gleichbedeutend mit der einen Kongruenz

$$\varphi(x) \equiv 0 \text{ mod. } \{p, R(x)\},$$

der auch, unter $\psi(x)$ eine ganze, ganzzahlige Funktion verstanden, die Form

$$\varphi(x) \equiv R(x) \cdot \psi(x) \text{ (mod. } p)$$

gegeben werden kann. Diese beweist, daß eine Kongruenz, welcher ϱ (mod. p) genügt, wenn sie nicht identisch ist, nicht geringeren Grades sein kann als n, demnach ist ϱ eine ganze Zahl des Körpers, wie sie als unter der gedachten Voraussetzung vorhanden nachgewiesen werden sollte, eine Zahl nämlich, für welche die Kongruenz niedrigsten Grades (mod. p), der sie genügt, vom n^{ten} Grade, nämlich die Kongruenz $R(x) \equiv 0$ (mod. p) ist, in deren Index folglich die Primzahl p nicht enthalten sein kann.

Auf Grund dieses zuerst von Dedekind gewonnenen Resultates (vgl. Theorie der Ideale und der höheren Kongruenzen, Götting. Abh. Bd. 23) läßt sich nun die Bedingung für die Existenz gemeinsamer außerwesentlicher Teiler noch auf eine andere Weise formulieren, als vorher geschehen ist. Denn nach diesem Dedekindschen Satze leuchtet ein, daß die Primzahl p dann und nur dann in dem Index jeder Zahl der Gattung $\mathfrak{G}$ enthalten sein wird, wenn r inkongruente

Primfunktionen $P_i(x)$ der bezüglichen Grade f_i (mod. p) nicht vorhanden sind. Nun beträgt die Anzahl aller inkongruenten Primfunktionen (mod. p), deren Grad f ist, wenn $a, b, c, \cdots$ die verschiedenen in f aufgehenden Primfaktoren bezeichnen, nach (72) des dritten Kapitels

$$\frac{1}{f} \cdot g(f),$$

wo

$$g(f) = p^f - \sum p^{\frac{f}{a}} + \sum p^{\frac{f}{ab}} - \cdots$$

ist. Wenn also die ungleichen der Gradzahlen $f_1, f_2, \cdots, f_r$ mit $f_1, f_2, \cdots, f_s$ bezeichnet werden, und die Anzahl derjenigen, welche gleich f_i sind, mit l_i, sodaß

$$l_1 + l_2 + \cdots + l_s = r$$

ist, so ist klar, daß unmöglich r Primfunktionen $P_i(x)$ der angegebenen Beschaffenheit vorhanden sein können, wenn auch nur eine der Ungleichheiten

$$l_i > \frac{1}{f_i} \cdot g(f_i) \qquad (64)$$
$$(i = 1, 2, \cdots, s)$$

erfüllt ist, während entgegengesetzten Falles solche r Primfunktionen immer angebbar sind. Mithin ist im ersten Falle und nur in ihm die Primzahl p ein gemeinsamer außerwesentlicher Teiler, und der Henselsche Satz läßt sich durch diesen andern ersetzen:

Damit eine Primzahl

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

deren Primidealfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ resp. von den Graden $f_1, f_2, \cdots, f_r$ sind, gemeinsamer außerwesentlicher Diskriminantenteiler sei, ist notwendig und hinreichend, daß von den Ungleichheiten (64) wenigstens eine erfüllt ist.

9. Immerhin bleibt es noch in Frage, ob es Körper gibt, in denen solche Primzahlen p wirklich vorhanden sind. Es ist daher ein besonderes Verdienst Dedekinds, einen derartigen Körper nachgewiesen zu haben.[1]) Indem wir dies sein

---

1) Dedekind, Götting. Anz. 20./9, 1871, sowie Götting. Abh. Bd. 23, p. 30.

Beispiel, sowie ein anderes von Hensel gegebenes zur Erläuterung der abgeleiteten beiden Kriterien hier anfügen wollen, müssen wir zunächst noch eines andern von dem Ersteren (a. a. O.) ausgesprochenen Satzes Erwähnung tun. Es fragt sich nämlich, wie man gegebenen Falles feststellen kann, ob eine bestimmte Primzahl im Index einer Zahl θ aufgehe oder nicht. Der Körper, welchem θ angehört, ist zumeist nur durch diese ihn erzeugende Zahl, die letztere aber durch die Gleichung gegeben, der sie genügt. Aus dieser findet sich dann freilich auch die Diskriminante der Zahl θ, und folglich würde ihr Index C und mit ihm zugleich auch dessen Primfaktoren durch die Beziehung

$$\Delta(1, \theta, \theta^2, \cdots, \theta^{n-1}) = C^2 \cdot \Delta(\mathfrak{g})$$

angebbar sein, falls die Grundzahl $\Delta(\mathfrak{g})$ des Körpers bekannt wäre. Dies ist aber zumeist nicht von vornherein der Fall. Deshalb ist es von Wert, die Primfaktoren des Index unabhängig von der Grundzahl ermitteln zu können, und dies ermöglicht der gedachte Dedekindsche Satz, den wir folgendermaßen aussprechen:

Man denke die Funktion $F(x)$, welche gleich Null gesetzt die Gleichung bildet, welche θ bestimmt, in ihre Primfaktoren (mod. p) zerlegt und nenne deren Produkt $\Pi(x)$, sodaß eine Gleichung besteht von der Form

$$F(x) = \Pi(x) - p \cdot M(x), \tag{65}$$

in welcher $M(x)$ eine ganze, ganzzahlige Funktion von x bedeutet. Die notwendige und hinreichende Bedingung dafür, daß der Index von θ durch p teilbar sei, besteht dann darin, daß $M(x)$ durch einen Primfaktor $P(x)$, welcher in $\Pi(x)$ mehrfach auftritt, ebenfalls teilbar sei (mod. p).

Um dies zu beweisen, betrachten wir zunächst eine Primzahl p, welche im Index von θ nicht aufgeht. Für eine solche stellt nach den Betrachtungen, aus denen wir den Dedekindschen Satz der vorigen Nummer herleiteten, die Kongruenz (55) die Zerlegung von $F(x)$ in Primfaktoren (mod. p), ihre rechte Seite also die vorher mit $\Pi(x)$ bezeichnete Funktion

dar, auch wissen wir bereits, daß $P_1(\theta)$ teilbar ist durch $\mathfrak{p}_1$, allgemeiner jedes $P_i(\theta)$ durch das entsprechende Ideal $\mathfrak{p}_i$ von p. Ferner kann aber keine dieser Zahlen $P_i(\theta)$ durch eins der von $\mathfrak{p}_i$ verschiedenen Primideale, noch auch, falls $e_i > 1$ ist, durch $\mathfrak{p}_i^2$ teilbar sein. Denn, wäre z. B. $P_1(\theta)$ teilbar durch $\mathfrak{p}_1^2$ und $e_1 > 1$, so würde gewiß

$$P_1(\theta)^{e_1-1} \cdot P_2(\theta)^{e_2} \cdots P_r(\theta)^{e_r}$$

durch p teilbar und somit θ schon eine Wurzel der Kongruenz

$$P_1(x)^{e_1-1} \cdot P_2(x)^{e_2} \cdots P_r(x)^{e_r} \equiv 0 \pmod{p}$$

sein, deren Grad doch kleiner ist als n, was für Primzahlen der betrachteten Art nicht möglich ist. Wäre aber etwa $P_1(\theta)$ teilbar noch durch $\mathfrak{p}_2$, so hätten die beiden Kongruenzen

$$P_1(x) \equiv 0, \ P_2(x) \equiv 0 \pmod{\mathfrak{p}_2}$$

eine gemeinsame Wurzel θ, während doch, da $P_1(x)$, $P_2(x)$ inkongruente Primfunktionen (mod. p) sind, eine Kongruenz von der Gestalt

$$P_1(x) \cdot F_1(x) + P_2(x) \cdot F_2(x) \equiv 1 \pmod{p}$$

also auch (mod. $\mathfrak{p}_2$) besteht, aus welcher die Unzulässigkeit jener zwei Kongruenzen für $x = \theta$ erhellt. Hieraus ist zu schließen, daß die Zahl $\Pi(\theta)$ jeden Primidealfaktor $\mathfrak{p}_i$ von p, für welchen $e_i > 1$ ist, genau ebenso oft enthält, wie p selbst. Da nun aus (65) für $x = \theta$ die Gleichung

$$0 = \Pi(\theta) - p \cdot M(\theta)$$

hervorgeht, so leuchtet ein, daß die Zahl $M(\theta)$ durch keins dieser Primideale $\mathfrak{p}_i$, also auch die Funktion $M(x)$ durch keine der entsprechenden Primfunktionen $P_i(x)$ (mod. p) teilbar sein kann, da aus einer Gleichung von der Form

$$M(x) = p \cdot \varphi(x) + P_i(x) \cdot \psi(x)$$

sich $M(\theta)$ durch $\mathfrak{p}_i$ teilbar ergäbe.

Man folgert also **erstens**, daß, wenn im Gegenteil die Funktion $M(x)$ durch eine in $\Pi(x)$ mehrfach auftretende Primfunktion (mod. p) teilbar ist, die Primzahl p im Index von θ aufgehen muß.

Ist aber umgekehrt p ein Teiler des Index der Zahl θ, so

gibt es (nach Nr. 6) n ganze, nicht sämtlich durch p teilbare Zahlen $x_1, x_2, \cdots, x_n$ von der Beschaffenheit, daß die Zahl

$$\varphi(\theta) = x_1 + x_2\theta + \cdots + x_n\theta^{n-1} \equiv 0 \pmod{p}$$

ist. Bezeichnet dann $A(x)$ den größten (mod. p) gemeinsamen Teiler der beiden Funktionen $\varphi(x)$, $F(x)$, der als Teiler von $\Pi(x)$ gedacht werden darf und von geringerem Grade wie $F(x)$ sein muß, so nimmt die Gleichung (65) die Gestalt

$$F(x) = A(x)\,B(x) - p\,M(x) \tag{66}$$

an, unter $B(x)$ eine ganze, ganzzahlige Funktion von x verstanden, die mindestens vom ersten Grade ist, also gewiß eine Primfunktion (mod. p) als Faktor besitzt, die wir $P(x)$ nennen wollen. Ferner gibt es zwei ganze, ganzzahlige Funktionen $\psi(x)$, $\chi(x)$ der Art, daß

$$F(x)\,\psi(x) + \varphi(x)\,\chi(x) \equiv A(x) \pmod{p}$$

ist; man folgert daher, daß $A(\theta)$ eine durch p teilbare ganze Zahl und als solche Wurzel einer Gleichung mit ganzzahligen Koeffizienten a_i von der Form

$$X^s + pa_1X^{s-1} + p^2a_2X^{s-2} + \cdots + p^sa_s = 0$$

ist. Demnach besteht die Identität

$$A(\theta)^s + pa_1 \cdot A(\theta)^{s-1} + \cdots + p^sa_s = 0,$$

welche, mit $B(\theta)^s$ multipliziert, in Beachtung der aus (66) folgenden Gleichheit

$$A(\theta)B(\theta) = pM(\theta)$$

die andere:

$$M(\theta)^s + a_1M(\theta)^{s-1} \cdot B(\theta) + \cdots + a_sB(\theta)^s = 0$$

liefert. Wegen der Irreduktibilität der Gleichung $F(x) = 0$, welcher die Zahl θ der Gattung $\mathfrak{G}$ genügt, ergeben sich aus diesen Formeln Beziehungen von der Form

$$A(x)^s + pa_1 \cdot A(x)^{s-1} + \cdots + p^sa_s = F(x)Q(x)$$
$$M(x)^s + a_1M(x)^{s-1} \cdot B(x) + \cdots + a_sB(x)^s = F(x)\,R(x).$$

Die erste derselben läßt sich als Kongruenz schreiben, wie folgt:

$$A(x)^s \equiv 0 \quad \text{mod. } \{p,\ F(x)\},$$

die zweite mit Rücksicht auf (66) folgendermaßen:

$$M(x)^s \equiv 0 \quad \text{mod. } \{p, B(x)\}.$$

Da nun der oben gedachte Primteiler $P(x)$ von $B(x)$ (mod. p) wegen (66) auch ein solcher von $F(x)$ ist, schließt man aus diesen Kongruenzen, daß $P(x)$ sowohl in $A(x)$ als auch in $M(x)$ (mod. p) aufgehen und des ersteren Umstandes wegen nach (66) ein mehrfacher Primteiler von $F(x)$ (mod. p) sein muß.

Also ergibt sich zweitens, daß, wenn p im Index von θ als Faktor enthalten ist, ein mehrfacher Primfaktor von $\Pi(x)$ vorhanden sein muß, der auch ein Teiler von $M(x)$ (mod. p) ist. Die beiden nunmehr von uns festgestellten Momente bilden aber zusammengenommen den Inhalt des behaupteten Satzes.

10. Nunmehr sei $\mathfrak{K}$ der Körper, welcher durch eine Wurzel θ der irreduktibeln kubischen Gleichung

$$F(x) = x^3 - x^2 - 2x - 8 = 0 \tag{67}$$

erzeugt wird. Ist $\delta(\theta)$ die Differente von θ, d. h.

$$\delta(\theta) = F'(\theta) = 3\theta^2 - 2\theta - 2, \tag{68}$$

so ist (vgl. Kap. 1, (74))

$$\Delta(1, \theta, \theta^2) = -N\delta(\theta). \tag{69}$$

Da aber durch Multiplikation der Gleichung (68) mit $1, \theta, \theta^2$ in Rücksicht auf die Identität

$$\theta^3 - \theta^2 - 2\theta - 8 = 0 \tag{70}$$

die drei Gleichungen

$$\begin{aligned} \delta(\theta) &= -2 - 2\theta + 3\theta^2 \\ \theta \cdot \delta(\theta) &= 24 + 4\theta + \theta^2 \\ \theta^2 \cdot \delta(\theta) &= 8 + 26\theta + 5\theta^2 \end{aligned}$$

erhalten werden, aus denen durch Elimination von θ die folgende:

$$\begin{vmatrix} -2 - \delta(\theta), & -2, & 3 \\ 24\ \ , & 4 - \delta(\theta), & 1 \\ 8\ \ , & 26, & 5 - \delta(\theta) \end{vmatrix} = 0$$

oder, entwickelt, diese andere:

$$\zeta(\theta)^3 - 7 \cdot \zeta(\theta)^2 - 2012 = 0$$

hervorgeht, so findet sich $N\zeta(\theta) = 2012$, mithin nach (69)

$$\Delta(1,\ \theta,\ \theta^2) = -\ 2^2 \cdot 503. \tag{71}$$

Nun geht das Quadrat des Index von θ in dieser Diskriminante auf, also kann der Index nur 1 oder 2, und die einzige Primzahl, die etwa in ihm aufgeht, $p = 2$ sein. Um dies zu erproben, suchen wir die Zerlegung der Funktion $F(x)$, welche in der Gestalt

$$F(x) = x^2(x-1) - 2 \cdot (x+4)$$

geschrieben werden kann, in ihre Primfaktoren (mod. 2). Wir erhalten, wenn

$$P_1(x) = x,\ P_2(x) = x - 1,\ M(x) = x + 4$$

gesetzt wird,

$$F(x) \equiv P_1(x)^2\, P_2(x) \quad (\text{mod. } 2),$$

während $M(x)$ (mod. 2) teilbar ist durch $P_1(x)$. Dem Satze der vorigen Nummer zufolge ist daher 2 ein Teiler des Index von θ, dieser Index selbst also gleich 2. Daraus folgt die Grundzahl des Körpers

$$\Delta(\mathfrak{g}) = -\ 503. \tag{72}$$

Setzt man nun

$$\eta = \tfrac{1}{2}\theta(\theta - 1) - 1$$

oder

$$2\eta = \theta^2 - \theta - 2, \tag{73}$$

so finden sich bei Beachtung der Identität (70) die beiden Gleichungen

$$2\eta\theta = 8,\quad 2\eta\theta^2 = 8\theta$$

und aus diesen und der vorigen Gleichung durch Elimination von θ die andere:

$$\eta^3 + \eta^2 + 2\eta - 8 = 0,$$

welche lehrt, daß η eine **ganze** Zahl des Körpers ist. Da ferner

$$\begin{aligned} 1 &= 1 \cdot 1 + 0 \cdot \theta + 0 \cdot \eta \\ \theta &= 0 \cdot 1 + 1 \cdot \theta + 0 \cdot \eta \\ \theta^2 &= 2 \cdot 1 + 1 \cdot \theta + 2 \cdot \eta \end{aligned}$$

gesetzt werden kann, erhält man

$$\Delta(1, \theta, \theta^2) = \begin{vmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 2, & 1, & 2 \end{vmatrix}^2 \cdot \Delta(1, \theta, \eta)$$

mithin wegen (71) und (72)

$$\Delta(1, \theta, \eta) = \Delta(\mathfrak{g}),$$

d. h. die Zahlen $1, \theta, \eta$ bilden eine Basis von $\mathfrak{g}$, oder jede ganze Zahl γ des Körpers hat die Gestalt

$$\gamma = x + \theta y + \eta z,$$

wo x, y, z rationale ganze Zahlen bedeuten. Hieraus folgt

$$\gamma^2 \equiv x^2 + \theta^2 y^2 + \eta^2 z^2 \pmod{2}$$

oder, da aus (73) leicht

$$\eta^2 = 2\theta - \eta - 2$$

also

$$\theta^2 \equiv \theta, \quad \eta^2 \equiv \eta \pmod{2}$$

gefunden wird, für jede Zahl γ in $\mathfrak{g}$ die Kongruenz

$$\gamma^2 \equiv \gamma \pmod{2}. \tag{74}$$

Diese lehrt, daß das Ideal $\mathfrak{g}2$ nur aus Primidealen ersten Grades zusammengesetzt sein kann, denn, heißt f der Grad eines darin aufgehenden Primideals $\mathfrak{p}$, so gibt es Zahlen γ, welche zum Exponenten f passen, derart, daß erst $\gamma^{2^f} \equiv \gamma \pmod{\mathfrak{p}}$ wäre; da aber wegen (74) schon $\gamma^2 \equiv \gamma \pmod{\mathfrak{p}}$ ist, muß $f = 1$ sein. Ein jedes jener Primideale kann aber auch nur einmal in $\mathfrak{g}2$ enthalten sein, denn, wäre $\mathfrak{g}2 = \mathfrak{p}^2 \cdot \mathfrak{q}$, mithin $\mathfrak{p}\mathfrak{q}$ nicht enthalten in $\mathfrak{g}2$, so gäbe es in $\mathfrak{p}\mathfrak{q}$ eine nicht durch 2 teilbare Zahl γ, deren Quadrat γ^2, weil in $\mathfrak{p}^2\mathfrak{q}^2$ enthalten, durch $\mathfrak{p}^2\mathfrak{q}$, d. i. durch 2 teilbar sein würde, eine Folgerung, welche mit der Kongruenz (74), der auch diese Zahl γ genügen müßte, unverträglich ist. Aus der Formel (25), in welcher hier $n = 3$ und die e_i, f_i gleich 1 zu denken sind, ergibt sich also, daß das Ideal

$$\mathfrak{g}2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$$

d. i. gleich dem Produkte aus drei verschiedenen Primidealen ersten Grades sein muß. Man bestätigt dieses Er-

gebnis durch Betrachtung der Fundamentalgleichung des Körpers. Ist nämlich

$$w_0 = u_1 + \theta u_2 + \eta u_3$$

die Fundamentalform desselben, eine Gleichung, für welche auch diese:

$$2w_0 = 2u_1 + 2\theta u_2 + (\theta^2 - \theta - 2)\, u_3$$

gesetzt werden kann, so findet sich mit einigem Aufwande von Rechnung als Fundamentalgleichung nachstehende Gleichung in w:

$$\begin{aligned} & w^3 - (3u_1 + u_2 - u_3)\, w^2 \\ & \quad + (3u_1^2 + 2u_1u_2 - 2u_1u_3 - 2u_2^2 - 13u_2u_3 + 2u_3^2)\, w \\ & \quad - (u_1^3 + u_1^2u_2 - u_1^2u_3 - 2u_1u_2^2 - 13u_1u_2u_3 + 2u_1u_3^2 \\ & \quad + 8u_2^3 - 6u_2^2u_3 + 10u_2u_3^2 + 8u_3^3) = 0. \end{aligned}$$

Als Kongruenz (mod. 2) aufgefaßt nimmt sie folgende einfache Gestalt an:

$$(w + u_1)(w + u_1 + u_2)(w + u_1 + u_3) \equiv 0 \pmod{2}$$

und läßt erkennen, daß die allgemein mit $F(w;\, u_1, u_2, \cdots, u_n)$ bezeichnete Funktion hier in drei Primfaktoren ersten Grades zerfällt, daß also das Ideal $\mathfrak{g}2$ aus drei Primidealfaktoren ebenfalls ersten Grades zusammengesetzt ist, welche durch die Ausdrücke

$$\begin{aligned} \mathfrak{p}_1 &\sim 2z + 2u_1 + \theta u_2 + \eta u_3 & &\sim 2u_1 + \theta u_2 + \eta u_3 \\ \mathfrak{p}_2 &\sim 2z + 2u_1 + (\theta + 1)\, u_2 + \eta u_3 & &\sim 2u_1 + (\theta + 1)\, u_2 + \eta u_3 \\ \mathfrak{p}_3 &\sim 2z + 2u_1 + \theta u_2 + (\eta + 1)\, u_3 & &\sim 2u_1 + \theta u_2 + (\eta + 1)\, u_3 \end{aligned}$$

oder, was hierfür gesetzt werden kann,

$$\begin{aligned} \mathfrak{p}_1 &= [2,\ \theta,\ \eta] \\ \mathfrak{p}_2 &= [2,\ \theta + 1,\ \eta] \\ \mathfrak{p}_3 &= [2,\ \theta,\ \eta + 1] \end{aligned}$$

dargestellt werden dürfen.

Nun beträgt aber die Anzahl inkongruenter Primfunktionen $P(x)$ ersten Grades (mod. 2) nur zwei; demnach schließt man aus dem allgemeinen Dedekindschen Satze der Nr. 8, daß in dem besonderen hier vorliegenden Körper die Primzahl 2 im Index jeder seiner ganzen Zahlen enthalten

oder ein gemeinsamer außerwesentlicher Teiler aller ihrer Diskriminanten sein muß.

11. Als zweites Beispiel[1]) betrachten wir den Körper, welcher durch die drei m-gliedrigen Perioden η_0, η_1, η_2 der p^{ten} Einheitswurzeln erzeugt wird, wenn $p = 3m + 1$ eine Primzahl ist. Wir bedienen uns dabei der Bezeichnungen und der Sätze, die in des Verfassers „die Lehre von der Kreisteilung etc." Vorlesung 11, Nr. 1 und 15, Nr. 4 benutzt bezw. entwickelt worden sind. Jede Primzahl p der angegebenen Form kann in der Gestalt

$$p = (a + b\varrho)(a + b\varrho^2) \tag{75}$$

geschrieben werden, wo ϱ die kubische Einheitswurzel $\frac{-1+\sqrt{-3}}{2}$ und a, b rationale ganze Zahlen bezeichnen, deren zweite ein Vielfaches von 3 ist; daraus folgt

$$4p = A^2 + 27B^2, \tag{76}$$

wenn

$$A = 2a - b,\ 3B = b \tag{77}$$

gesetzt wird; auch weiß man, daß diese Zerlegung der Zahl $4p$ in die Summe einer Quadratzahl und das 27fache einer solchen nur auf eine Weise möglich ist. Da die drei Perioden durch eine beliebige von ihnen, etwa durch η_0 rational ausgedrückt werden können, so ist der aus ihnen erzeugte Körper $\mathfrak{K}$ kein anderer, als der aus η_0 erzeugte. Die erzeugende Gleichung aber ist die Gleichung, welcher die drei Perioden Genüge leisten, nämlich (s. Kreisteilung p. 213) die Gleichung

$$x^3 + x^2 - \frac{p-1}{3}x - \frac{1}{9}\left(p\alpha + \frac{p-1}{3}\right) = 0, \tag{78}$$

worin die Zahl α mit der Zahl A durch die Formel

$$A = 3\alpha - 2 \tag{79}$$

verbunden ist. Hiernach finden sich für die Differente $\partial(\eta_0)$ der Zahl η_0 die folgenden Gleichungen:

---

1) Hensel, Journ. f. Math. 113 „arithmetische Untersuchungen über die gemeinsamen außerwesentlichen Diskriminantenteiler einer Gattung" § 3.

$$\varepsilon(\eta_0) = 3\eta_0^2 + 2\eta_0 - \frac{p-1}{3}$$

$$\eta_0 \cdot \varepsilon(\eta_0) = -\eta_0^2 + 2\cdot\frac{p-1}{3}\eta_0 + 3C$$

$$\eta_0^2 \cdot \varepsilon(\eta_0) = \left(1 + 2\cdot\frac{p-1}{3}\right)\eta_0^2 + \left(3C - \frac{p-1}{3}\right)\eta_0 - C,$$

in denen zur Abkürzung $\frac{1}{9}\left(p\alpha + \frac{p-1}{3}\right) = C$ gesetzt ist. Aus ihnen ergibt sich die Norm der Differente und nach Kap. 1, Formel (74) die Diskriminante von η_0, nämlich

$$\Delta(1, \eta_0, \eta_0^2) = \begin{vmatrix} 3, & 2, & -\frac{p-1}{3} \\ -1, & 2\cdot\frac{p-1}{3}, & 3C \\ 1+2\cdot\frac{p-1}{3}, & 3C-\frac{p-1}{3}, & -C \end{vmatrix},$$

eine Gleichung, welche auf die einfache Form

$$(80) \qquad \Delta(1, \eta_0, \eta_0^2) = -B^2 \cdot p^2$$

gebracht werden kann. Da andererseits die Gleichungen bestehen:

$$1 = -\eta_0 - \eta_1 - \eta_2$$
$$\eta_0 = 1\cdot\eta_0 + 0\cdot\eta_1 + 0\cdot\eta_2$$
$$\eta_0^2 = \left(\frac{p-1}{3} - m_0^0\right)\eta_0 + \left(\frac{p-1}{3} - m_1^0\right)\eta_1 + \left(\frac{p-1}{3} - m_2^0\right)\eta_2,$$

wo m_0^0, m_1^0, m_2^0 (vgl. Kreisteilung p. 201, (4)) drei ganze Zahlen bezeichnen, welche die Bedingung

$$m_1^0 - m_2^0 = B$$

erfüllen, so folgt die Beziehung

$$\Delta(1, \eta_0, \eta_0^2) = \begin{vmatrix} -1, & -1, & -1 \\ 1, & 0, & 0 \\ \frac{p-1}{3} - m_0^0, & \frac{p-1}{3} - m_1^0, & \frac{p-1}{3} - m_2^0 \end{vmatrix}^2 \cdot \Delta(\eta_0, \eta_1, \eta_2)$$

d. i. einfacher

$$\Delta(1, \eta_0, \eta_0^2) = B^2 \cdot \Delta(\eta_0, \eta_1, \eta_2).$$

Mit Rücksicht auf (80) findet sich also

$$\Delta(\eta_0, \eta_1, \eta_2) = -p^2.$$

Da nun jede Diskriminante ganzer Zahlen von der Grundzahl des Körpers nur um einen quadratischen Faktor, die Grundzahl selbst aber, wie später (Kap. 8, Nr. 6) gezeigt werden wird, stets von ± 1 verschieden ist, so lehrt vorstehende Gleichung, daß $-p^2$ die Grundzahl des Körpers $\mathfrak{K}$ und das System η_0, η_1, η_2 eine Basis für die Gesamtheit $\mathfrak{g}$ seiner ganzen Zahlen darstellt. Demgemäß darf

$$w_0 = \eta_0 u_0 + \eta_1 u_1 + \eta_2 u_2$$

als Fundamentalform angesetzt werden, deren konjugierte Formen dann bekanntlich

$$w_0^{(1)} = \eta_1 u_0 + \eta_2 u_1 + \eta_0 u_2$$
$$w_0^{(2)} = \eta_2 u_0 + \eta_0 u_1 + \eta_1 u_2$$

sind. Die Diskriminante der Fundamentalgleichung wird mithin das Quadrat des Differenzenproduktes

$$(w_0 - w_0^{(1)})\,(w_0^{(1)} - w_0^{(2)})\,(w_0^{(2)} - w_0),$$

welches durch Substitution der vorigen Ausdrücke und mit Rücksicht auf die Koeffizienten der kubischen Gleichung (78), sowie auf die Gleichung (75) sich in die Form

$$(81) \qquad -p(a\,U_1 + B\,U_2)$$

bringen läßt, wenn zur Abkürzung

$$u_0 u_1^2 + u_1 u_2^2 + u_2 u_0^2 - u_0^2 u_1 - u_1^2 u_2 - u_2^2 u_0 = U_1$$
$$u_0^3 + u_1^3 + u_2^3 + 6 u_0 u_1 u_2 - 3(u_0 u_1^2 + u_1 u_2^2 + u_2 u_0^2) = U_2$$

gesetzt wird. Der Formel (52) gemäß und nach dem zuvor gefundenen Werte der Grundzahl $\Delta(\mathfrak{g})$ findet sich daher die Gleichung

$$\vartheta(u_0, u_1, u_2) = a\,U_1 + B\,U_2.$$

Um nun zu untersuchen, ob die Primzahl 2 gemeinsamer außerwesentlicher Teiler aller Diskriminanten der vorliegenden Gattung algebraischer Zahlen sei, muß die vorbezeichnete Funktion in bezug auf den Modulus

$$\{2,\ u_0^2 - u_0,\ u_1^2 - u_1,\ u_2^2 - u_2\}$$

untersucht werden. Offenbar ergibt sich aber in bezug auf denselben

$$U_1 \equiv 0,$$
$$U_2 \equiv u_0 + u_1 + u_2 + u_0 u_1 + u_1 u_2 + u_2 u_0$$

und folglich

$$\vartheta(u_0, u_1, u_2) \equiv B(u_0 + u_1 + u_2 + u_0 u_1 + u_1 u_2 + u_2 u_0),$$

demnach dann und nur dann bei unbestimmt bleibenden u_i kongruent Null, wenn B durch 2 teilbar ist, was nach den Gleichungen (77) dann und nur dann zutrifft, wenn zugleich auch A es ist, der Gleichung (76) zufolge also p eine Zerlegung zuläßt von der Form

$$p = A'^2 + 27 B'^2.$$

Man erhält demnach folgenden eleganten Satz: In dem betrachteten Körper $\mathfrak{K}$ ist die Primzahl 2 dann und nur dann ein gemeinsamer außerwesentlicher Diskriminantenteiler, wenn die Primzahl p von der Form $3m+1$ eine Zerlegung in eine Quadratzahl und das 27fache einer Quadratzahl gestattet. Dies trifft für die fraglichen Primzahlen der beiden ersten Hundert nur zu bei

$$p = 31,\ 43,\ 109,\ 127,\ 157,\ 189.$$

12. Aus diesen Betrachtungen ersieht man, daß es Körper gibt, in denen die Funktion

$$\vartheta\,(u_1, u_2, \cdots, u_n),$$

obwohl sie als Funktion der Unbestimmten u_i keinen Zahlenteiler hat, doch für alle ganzzahligen Wertsysteme dieser Größen einen und denselben Teiler erhalten kann. *Kronecker* hat aber auf den beachtenswerten Umstand aufmerksam gemacht, daß alsdann ein Zahlenkörper angebbar ist von der Beschaffenheit, daß, wenn den Unbestimmten u_i nicht nur alle Systeme rationaler ganzer Zahlen, sondern allgemeiner alle Systeme ganzer Zahlen α_i dieses Körpers beigelegt werden, ein mit p gemeinsamer Teiler aller so entstehenden Werte $\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ nicht mehr vorhanden ist. In derselben Arbeit, der wir das zweite Beispiel entnahmen, hat Hensel die Kroneckersche Aussage bestätigt, indem er den Zahlenkörper niedrigsten Grades, für den das Gesagte zutrifft, be-

stimmt hat. Um auch von dieser interessanten Untersuchung Mitteilung zu machen, müssen wir zunächst dem Hilfssatze in Nr. 8 des dritten Kapitels eine entsprechende größere Ausdehnung geben. Der dort gegebene Beweis des Satzes beruht wesentlich darauf, daß die rationalen ganzen Zahlen $x, y, z, \cdots$ (mod. p) die sämtlichen Wurzeln der Kongruenzen

$$x^p - x \equiv 0, \; y^p - y \equiv 0, \; z^p - z \equiv 0, \; \cdots \; (\text{mod. } p)$$

ausmachen, und daß die Anzahl der Wurzeln jeder dieser Kongruenzen gleich p, nämlich gleich ihrem Grade ist. Man wird deshalb den Satz sogleich folgendermaßen verallgemeinert aussprechen können:

Damit eine ganze, ganzzahlige Funktion

$$F(u_1, u_2, \cdots, u_n) \tag{82}$$

für alle Wurzeln der ganzzahligen Kongruenzen

$$F_1(u_1) \equiv 0, \; F_2(u_2) \equiv 0, \; \cdots, \; F_n(u_n) \equiv 0 \; (\text{mod. } p), \tag{83}$$

deren eine jede genau soviel habe, als ihr Grad beträgt, durch p teilbar werde, ist notwendig und hinreichend, daß jene Funktion in dem Modulus

$$\{p, \; F_1(u_1), \; F_2(u_2), \; \cdots, \; F_n(u_n)\} \tag{84}$$

enthalten sei.

Ist nun aber $K(\alpha; R)$ irgend ein Körper, π ein demselben angehöriger Primidealfaktor von p, so beweist sich in gleicher Weise der noch allgemeinere Satz, daß eine Funktion $F(u_1, u_2, \cdots, u_n)$, deren Koeffizienten ganze Zahlen des Körpers sind, dann und nur dann für alle derartigen Wurzeln der Kongruenzen

$$F_1(u_1) \equiv 0, \; F_2(u_2) \equiv 0, \; \cdots, \; F_n(u_n) \equiv 0 \; (\text{mod. } \pi), \tag{85}$$

deren jede ihrer soviel haben soll, als ihr Grad beträgt, durch π teilbar sein werde, wenn sie in dem Modulus

$$\{\pi, \; F_1(u_1), \; F_2(u_2), \; \cdots, \; F_n(u_n)\} \tag{86}$$

enthalten ist. Reduziert man jedoch unter der besonderen Voraussetzung, daß die Funktion F und die Funktionen F_i rational ganzzahlige Koeffizienten haben, die erstgenannte Funktion zunächst in bezug auf das Modulsystem $\{F_1, F_2, \cdots, F_n\}$,

so leuchtet ein, daß der bezügliche Rest ebenfalls eine Funktion mit rational ganzzahligen Koeffizienten sein muß und folglich dann und nur dann durch π teilbar ist, wenn er es ist durch p. In dieser besonderen Voraussetzung wird demnach die Funktion $F(u_1, u_2, \cdots, u_n)$ dann und nur dann für alle Systeme von Wurzeln der Kongruenzen (85) teilbar sein durch π, wenn sie statt in dem Modulus (86), im Modulus

$$\{p, F_1(u_1), F_2(u_2), \cdots, F_n(u_n)\}$$

enthalten ist.

Nun bezeichne φ den Grad des Primideals π; dann werden die ganzzahligen Kongruenzen

$$u_1^{p^\varphi} - u_1 \equiv 0,\ u_2^{p^\varphi} - u_2 \equiv 0,\ \cdots,\ u_n^{p^\varphi} - u_n \equiv 0 \pmod{\pi}$$

genau soviel Wurzeln haben, welche ganze Zahlen des Körpers $K(\alpha; R)$ sind, als ihr Grad beträgt, und alle diese ganzen Zahlen des Körpers (mod. π) mit ihnen übereinstimmen. Nimmt man also für $F_i(u_i)$ die Funktion $u_i^{p^\varphi} - u_i$, so fließt zunächst aus dem vorigen Satze die Folgerung:

Damit die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ für alle Systeme ganzer Zahlen u_i des Körpers $K(\alpha; R)$ durch π teilbar werde, ist notwendig und hinreichend, daß sie in dem Modulus

$$P = \{p, u_1^{p^\varphi} - u_1, \cdots, u_n^{p^\varphi} - u_n\}$$

enthalten sei. Ist sie letzteres nicht, so gibt es also sicher ein System ganzer Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$ jenes Körpers von der Beschaffenheit, daß $\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ durch π nicht teilbar ist.

Dies vorausgeschickt, wollen wir festzustellen suchen, wann es ein System ganzer Zahlen des Körpers $K(\alpha; R)$ gebe, welches für die Unbestimmten u_i gesetzt die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ relativ prim macht zu p. Hierzu sei, in Primideale dieses Körpers zerlegt,

$$p = \pi_1^{e_1} \cdot \pi_2^{e_2} \cdots \pi_\varrho^{e_\varrho}, \tag{87}$$

und $\varphi_1, \varphi_2, \cdots, \varphi_\varrho$ die Gradzahlen der Ideale $\pi_1, \pi_2, \cdots, \pi_\varrho$; ihnen entsprechen ϱ Moduln

$$P_i = \{p, u_1^{p^{\varphi_i}} - u_1, \cdots, u_n^{p^{\varphi_i}} - u_n\}, \tag{88}$$

von denen jedoch nur diejenigen verschieden sind, welche ungleichen Gradzahlen zugehören. Aus den Vorbemerkungen folgt offenbar, daß, wenn die Funktion

$$\vartheta(u_1, u_2, \cdots, u_n)$$

auch nur in einem einzigen dieser Moduln enthalten ist, der ihm entsprechende Primidealfaktor von p ein gemeinsamer außerwesentlicher Diskriminantenteiler verbleibt; soll also ein Wertsystem der u_i innerhalb des Körpers $K(\alpha; R)$ vorhanden sein, welches $\vartheta(u_1, u_2, \cdots, u_n)$ prim gegen p macht, so darf diese Funktion in keinem der Moduln (88) enthalten sein. Diese notwendige Bedingung aber genügt auch. Denn, wenn sie erfüllt ist, gibt es für jedes der Primideale π_i ein Wertsystem $\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)}$ innerhalb jenes Körpers, der Art, daß

$$\vartheta(\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)})$$

nicht teilbar ist durch π_i. Wählt man dann innerhalb des Körpers, was möglich ist, die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$ so, daß

$$\alpha_k \equiv \alpha_k^{(1)} \pmod{\pi_1}, \ \alpha_k \equiv \alpha_k^{(2)} \pmod{\pi_2}, \cdots, \ \alpha_k \equiv \alpha_k^{(\varrho)} \pmod{\pi_\varrho}, \quad (k = 1, 2, \cdots, n)$$

woraus

$$\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n) \equiv \vartheta(\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots, \alpha_n^{(i)}) \pmod{\pi_i} \quad (i = 1, 2, \cdots, \varrho)$$

folgt, so ist der Funktionswert $\vartheta(\alpha_1, \alpha_2, \cdots, \alpha_n)$, weil durch keins der Primideale π_i teilbar, relativ prim gegen p, wie es verlangt wird. Man darf daher als nächstes Resultat dieser Betrachtungen den Satz aussprechen:

Damit der Körper $K(\alpha; R)$ leiste, was beabsichtigt ist, nämlich die Eigenschaft habe, daß die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ nicht für alle ihm angehörigen Systeme ganzer Zahlen $u_i = \alpha_i$ einen mit p gemeinsamen Teiler erhalte, sondern wenigstens für eins derselben relativ prim sei gegen p, ist notwendig und hinreichend, daß die Funktion in keinem der Moduln (88) enthalten sei. Hensel bezeichnet alsdann den Körper $K(\alpha; R)$ als einen Ergänzungskörper mit bezug auf p für den der Betrachtung zum Grunde liegenden Körper $K(\mathsf{A}; R)$.

Zum Nachweise aber von der Existenz eines derartigen Körpers und zugleich, um den Ergänzungskörper

niedrigsten Grades zu finden, haben wir folgendes zu bemerken. In der unbegrenzten Reihe der Moduln

$$(89)\qquad \Pi_i = \{p,\ u_1^{p^i} - u_1,\ u_2^{p^i} - u_2,\ \cdots,\ u_n^{p^i} - u_n\} \quad (i = 1, 2, 3, \cdots)$$

wird es einen ersten geben, in welchem die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ nicht enthalten ist. Denn, wenn p überhaupt kein gemeinsamer außerwesentlicher Diskriminantenteiler ist, so ist sie schon in Π_1 nicht enthalten (nach dem Satze in Nr. 8); wählt man aber k als die kleinste Zahl, für welche $p^k > \frac{n(n-1)}{2}$ ist, eine Zahl, die den Grad der Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ bezeichnet, so leuchtet ein, daß diese Funktion nicht mehr im Modulus Π_k enthalten sein kann, da sie sonst, weil nur Potenzen der Unbestimmten geringeren Grades als p^k enthaltend, einer mit p multiplizierten ganzen Funktion dieser Unbestimmten gleich sein müßte, während sie doch keinen Zahlenfaktor besitzt (Nr. 7). Nennen wir nun Π_φ den *ersten* der Moduln (89), in welchem die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ nicht mehr enthalten ist, und verstehen unter

$$(90)\qquad P(x) \equiv 0 \pmod{p}$$

irgend eine der (mod. p) irreduktibeln Kongruenzen φ^{ten} Grades. Dann wird der Körper $K(\alpha; R)$, der von einer Wurzel α der Gleichung $P(x) = 0$ erzeugt wird, der Ergänzungskörper niedrigsten Grades in bezug auf die Primzahl p sein. Zum Beweise stellen wir zunächst fest, daß er überhaupt solch Ergänzungskörper ist. In der Tat, da p in jenem Körper selbst Primzahl (s. Kap. 6, Nr. 21, Anfang), d. h. $\mathfrak{g}p$ ein Primideal π und seine Norm gleich p^φ, mithin φ der Grad von π ist, so könnte die Funktion $\vartheta(u_1, u_2, \cdots, u_n)$ nur dann für alle Systeme ganzer Zahlen $u_i = \alpha_i$ des gedachten Körpers durch π teilbar sein, wenn sie im Modulus Π_φ enthalten wäre; dies ist aber nach der Voraussetzung nicht der Fall. — Zudem gibt es aber auch keinen Ergänzungskörper niedrigeren Grades als den Körper $K(\alpha; R)$; denn, wäre $K(\beta; R)$ ein solcher vom Grade $\chi < \varphi$, und π ein Primidealfaktor von p in demselben, so könnte der Grad des letztern höchstens gleich

dem Grade χ des Körpers sein; da nun $\vartheta(u_1, u_2, \cdots, u_n)$ nach der Voraussetzung in jedem Modulus Π_i für $i \lessgtr \chi$ enthalten ist, würde den obigen Ergebnissen zufolge das Primideal π ein Teiler aller Funktionswerte sein, welche den Systemen ganzer Zahlen $u_i = \beta_i$ des letztgenannten Körpers entsprechen, und sonach dieser Körper kein Ergänzungskörper sein. Man ersieht hieraus ferner, daß solch Körper auch nur einer Gleichung φ^{ten} Grades, welche (mod. p) *irreduktibel* ist, entspringen kann, da andernfalls p in ihm aus mehreren Primidealfaktoren zusammengesetzt und deren Grad geringer sein müßte als φ, weshalb dem eben Bemerkten gemäß der Körper kein Ergänzungskörper sein könnte.

Endlich ist für den Ergänzungskörper niedrigsten Grades die besondere Wahl der Funktion $P(x)$ unter den (mod. p) irreduktibeln Funktionen φ^{ten} Grades ganz gleichgültig. Denn, ist $P'(x)$ irgend eine andere solche Funktion, so sind nach Kap. 3, Nr. 7 die Wurzeln der Kongruenz

$$P'(x) \equiv 0 \text{ (mod. } p)$$

ganze, ganzzahlige Funktionen von α; die Zahlen des Körpers $K(\alpha'; R)$, welcher aus der Wurzel α' der Gleichung $P'(x) = 0$ entspringt, werden daher (mod. p) den Zahlen des Körpers $K(\alpha; R)$, wie selbstverständlich auch umgekehrt, kongruent sein, und daher können bei der Frage nach den Primteilern von p, welche allen Werten von $\vartheta(u_1, u_2, \cdots, u_n)$ gemeinsam sind, die für die u_i zu nehmenden Zahlen des einen Körpers durch Zahlen des andern und umgekehrt ersetzt werden. Die, den verschiedenen (mod. p) irreduktibeln Funktionen φ^{ten} Grades entsprechenden Ergänzungskörper niedrigsten Grades können also mit bezug auf den Zweck, welchem sie dienen sollen, als ein- und derselbe gelten.

Hensel hat a. a. O. diesen Sätzen noch weitere Betrachtungen folgen lassen, welche auf die Bestimmung der Ergänzungskörper niedrigsten Grades von besonderer Beschaffenheit, z. B. solcher, welche aus Einheitswurzeln gebildet sind, u. dgl. Bezug haben; um aber nicht zu ausführlich zu werden, wollen wir uns damit begnügen, auf diese weiteren Punkte hier nur hinzuweisen.

13. Haben wir bisher von den außerwesentlichen Diskriminantenteilern gehandelt, so ist es nun an der Zeit, die wesentlichen Teiler, d. i. die rationalen Primzahlen zu untersuchen, welche in der allen Diskriminanten der Zahlen θ der Gattung $\mathfrak{G}$ als Faktor gemeinsamen Grundzahl $D = \Delta(\mathfrak{g})$ enthalten sind. Die Formel (52), in welcher die Funktion

$$\vartheta(u_1, u_2, \cdots, u_n)$$

eine Einheitsform bezeichnet, lehrt, daß die Teiler der Grundzahl mit denjenigen der Diskriminante $\Delta(1, w_0, w_0^2, \cdots, w_0^{n-1})$ der Fundamentalgleichung identisch und daher mittels des Ausdrucks der letzteren bestimmbar sind. Zu diesem Zwecke kehren wir zur Fundamentalgleichung $F(w) = 0$ und zu der Zerlegung der Funktion $F(w)$ in ihre irreduktibeln Faktoren in bezug auf eine gegebene Primzahl p zurück. Wird wieder, in Primidealfaktoren zerlegt,

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r} \tag{91}$$

angenommen, so lautet jene Zerlegung nach (45), wie folgt:

$$F(w) \equiv \mathfrak{F}_1(w)^{e_1}\mathfrak{F}_2(w)^{e_2}\cdots\mathfrak{F}_r(w)^{e_r} \pmod{p},$$

eine Kongruenz, aus welcher durch Differenzierung nach w die andere:

$$F'(w) \equiv \mathfrak{F}_1(w)^{e_1-1}\cdots\mathfrak{F}_r(w)^{e_r-1}\cdot\Phi(w) \pmod{p}$$

oder die Gleichung

$$F'(w) = \mathfrak{F}_1(w)^{e_1-1}\cdots\mathfrak{F}_r(w)^{e_r-1}\cdot\Phi(w) + p\cdot\Psi(w)$$

hervorgeht; dabei bedeutet $\Psi(w)$ eine ganze, ganzzahlige Funktion von w und den Unbestimmten u_i, während

$$\Phi(w) = e_1\cdot\mathfrak{F}_2(w)\cdots\mathfrak{F}_r(w) + e_2\cdot\mathfrak{F}_1(w)\mathfrak{F}_3(w)\cdots\mathfrak{F}_r(w) + \cdots$$

gesetzt ist. Wir nehmen zuerst an, daß keiner der Exponenten $e_1, e_2, \cdots, e_r$ durch p teilbar sei. Dann ist $\Phi(w)$ durch keine der Funktionen $\mathfrak{F}_1(w), \mathfrak{F}_2(w), \cdots, \mathfrak{F}_r(w)$ (mod. p) teilbar, da z. B. durch $\mathfrak{F}_1(w)$ alle Glieder dieses Ausdrucks vom zweiten an teilbar, das erste Glied aber weder durch p noch durch $\mathfrak{F}_1(w)$ teilbar ist, weil die Funktionen dieses Gliedes von $\mathfrak{F}_1(w)$ verschiedene, (mod. p) irreduktible Funktionen bedeuten. Hieraus folgt aber, daß $\Phi(w_0)$ durch keins der Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ aufgeht, folglich relativ

prim ist gegen p. Da infolge davon das erste Glied zur Rechten der Gleichung

$$\mathrm{F}'(w_0) = \mathfrak{F}_1(w_0)^{e_1-1} \cdots \mathfrak{F}_r(w_0)^{e_r-1} \cdot \Phi(w_0) + p \cdot \Psi(w_0)$$

genau durch $\mathfrak{p}_1^{e_1-1} \cdot \mathfrak{p}_2^{e_2-1} \cdots \mathfrak{p}_r^{e_r-1}$ aufgeht, während das zweite mindestens durch $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$ teilbar ist, so ergibt sich

$$\mathrm{F}'(w_0) = \mathfrak{p}_1^{e_1-1}\mathfrak{p}_2^{e_2-1} \cdots \mathfrak{p}_r^{e_r-1} \cdot G(u_1, u_2, \cdots, u_n),$$

unter $G(u_1, u_2, \cdots, u_n)$ eine ganze Funktion der Unbestimmten u_i verstanden, deren Koeffizienten dem Körper angehörige Ideale sind, aber keinen mit p gemeinsamen Idealteiler mehr haben. Durch den Übergang zur Norm liefert diese Gleichung, wenn man bedenkt, daß $N\mathrm{F}'(w)$ mit der Diskriminante der Fundamentalgleichung bis auf das Vorzeichen identisch ist, die andere:

$$\Delta(\mathfrak{g}) \cdot \vartheta(u_1, u_2, \cdots, u_n)^2 = p^{f_1(e_1-1)} \cdots p^{f_r(e_r-1)} \cdot H(u_1, u_2, \cdots, u_n),$$

in welcher die ganze Funktion $H(u_1, u_2, \cdots, u_n)$ rational ganzzahlige, nicht sämtlich durch p teilbare Koeffizienten haben wird. Demnach muß die Grundzahl $\Delta(\mathfrak{g})$ den Primfaktor p genau

$$f_1(e_1-1) + f_2(e_2-1) + \cdots + f_r(e_r-1) \tag{92}$$

Mal enthalten. — Wäre zweitens einer der Exponenten $e_1, e_2, \cdots, e_r$, etwa e_1 teilbar durch p, so wäre die Funktion $\Phi(w)$ (mod. p) teilbar durch $\mathfrak{F}_1(w)$, mithin $\Phi(w_0)$ teilbar durch $\mathfrak{p}_1$ und somit ginge der oben geschriebene Ausdruck für $\mathrm{F}'(w_0)$ mindestens durch

$$\mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2-1} \cdots \mathfrak{p}_r^{e_r-1}$$

und daher die Grundzahl $\Delta(\mathfrak{g})$ mindestens durch

$$p^{f_1 e_1 + f_2(e_2-1) + \cdots + f_r(e_r-1)}$$

auf. Man erhält daher das folgende wichtige Ergebnis:

Ist die Primzahl p nach der Formel (91) in Primidealfaktoren zerlegt, deren Gradzahlen resp.

$$f_1, f_2, \cdots, f_r$$

sind, so geht sie in der Grundzahl des Körpers mindestens so oft auf, wie die Zahl (92) angibt, und zwar genau so oft, falls keiner der Exponenten $e_1, e_2, \cdots, e_r$ durch p teilbar ist, entgegengesetzten Falls öfter.

Der erstere Fall findet aber immer statt, sobald p aus lauter verschiedenen Primidealen zusammengesetzt, nämlich jeder der Exponenten e_i gleich 1 ist; da alsdann der Ausdruck (92) sich auf Null reduziert, tritt keine derartige Primzahl p in der Grundzahl als Faktor auf; für jede Primzahl aber, die wenigstens einen Primidealfaktor mehrfach hat, ist jener Ausdruck von Null verschieden. Somit fließt aus dem vorigen Satze der einfachere, aber auch weniger scharfe Ausspruch: Die Grundzahl des Körpers ist ausschließlich aus all' denjenigen Primzahlen p zusammengesetzt, welche mehrfache Primidealfaktoren besitzen. Zudem erhellt hieraus, daß es von derartigen Primzahlen p nur eine endliche Menge gibt.

14. Die soeben nach *Hensel* abgeleiteten Sätze sind zuerst von *Dedekind* bewiesen worden. Die Bedeutung, welche ihnen zukommt, aber auch das Interesse, welches die Dedekindschen Entwicklungen an sich selbst darbieten, machen es wünschenswert, auch seinen Beweisen hier Raum zu gewähren. Der Beweis des unbestimmteren Ausspruchs über die Zusammensetzung der Grundzahl ist verhältnismäßig einfach und kann ohne größere Vorbereitungen geliefert werden.

I. Zunächst soll gezeigt werden, daß jede Primzahl p, die durch das Quadrat eines Primideals teilbar ist, ein Teiler der Grundzahl ist. Wenn nämlich $\mathfrak{g}p = \mathfrak{p}^2 \cdot \mathfrak{q}$ ist, so wird es eine im Ideale $\mathfrak{p}\mathfrak{q}$ enthaltene Zahl

$$\gamma = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_n\gamma_n$$

geben, welche nicht in $\mathfrak{p}^2\mathfrak{q}$ enthalten, d. h. nicht durch p teilbar ist, derart, daß nicht sämtliche Koeffizienten $c_1, c_2, \cdots, c_n$ durch p aufgehen; da aber γ^2 in $\mathfrak{p}^2\mathfrak{q}^2$ also auch in $\mathfrak{p}^2\mathfrak{q}$ enthalten ist, so muß dann γ^2 und folglich auch γ^p durch p teilbar sein. Nun ist

$$\gamma^p \equiv c_1\gamma_1^p + c_2\gamma_2^p + \cdots + c_n\gamma_n^p \pmod{p},$$

mithin muß die Kongruenz

$$c_1\gamma_1^p + c_2\gamma_2^p + \cdots + c_n\gamma_n^p \equiv 0 \pmod{p}$$

und daher auch alle ihr konjugierten Kongruenzen:

$$\left.\begin{array}{l} c_1\gamma_1^{(1)p} + c_2\gamma_2^{(1)p} + \cdots + c_n\gamma_n^{(1)p} \equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ c_1\gamma_1^{(n-1)p} + c_2\gamma_2^{(n-1)p} + \cdots + c_n\gamma_n^{(n-1)p} \equiv 0 \end{array}\right\} (\text{mod. } p)$$

erfüllt sein, was erfordert, daß die Diskriminante

$$(93) \qquad \varDelta(\gamma_1^p, \gamma_2^p, \cdots, \gamma_n^p) \equiv 0 \ (\text{mod. } p)$$

ist. Nun sieht man leicht ein, daß diese Diskriminante (mod. p) mit der Grundzahl

$$\varDelta(\mathfrak{g}) = \varDelta(\gamma_1, \gamma_2, \cdots, \gamma_n)$$

kongruent ist. Zu diesem Zwecke mag man z. B. bemerken, daß nach Kap. 1, Nr. 14 die letztbezeichnete Diskriminante gleich der Determinante

$$(94) \qquad \begin{vmatrix} S(\gamma_1\gamma_1), & S(\gamma_1\gamma_2), & \cdots, & S(\gamma_1\gamma_n) \\ S(\gamma_2\gamma_1), & S(\gamma_2\gamma_2), & \cdots, & S(\gamma_2\gamma_n) \\ \cdot & \cdot & \cdot & \cdot \\ S(\gamma_n\gamma_1), & S(\gamma_n\gamma_2), & \cdots, & S(\gamma_n\gamma_n) \end{vmatrix}$$

ist, während jene aus ihr entsteht, indem die γ_i durch ihre p^{ten} Potenzen ersetzt werden, daß aber zugleich allgemein für die Spur irgend einer ganzen Zahl ω des Körpers die Kongruenz

$$S(\omega)^p \text{ d. i. } (\omega + \omega^{(1)} + \cdots + \omega^{(n-1)})^p \equiv S(\omega^p) \ (\text{mod. } p)$$

besteht, sodaß durch die gedachte Substitution jene Determinante sich nur in einen mit ihrer p^{ten} Potenz und folglich mit ihr selbst (mod. p) kongruenten Ausdruck verwandeln kann. Aus (93) folgt demnach die Kongruenz

$$\varDelta(\mathfrak{g}) \equiv 0 \ (\text{mod. } p),$$

w. z. b. w.

II. Nicht ganz so leicht ist die Umkehrung zu beweisen, daß nämlich jede Primzahl p, welche ein Teiler der Grundzahl ist, durch das Quadrat eines Primideals teilbar sei. Hierzu denken wir uns die Grundzahl $\varDelta(\mathfrak{g})$ in Gestalt der Determinante (94). Ist diese Determinante, deren einzelne Elemente rationale ganze Zahlen sind, durch p teilbar, so gibt es rationale ganze Zahlen $x_1, x_2, \cdots, x_n$, die nicht sämtlich durch p aufgehen und von der Art, daß die n Kongruenzen:

$$x_1 S(\gamma_1 \gamma_i) + x_2 S(\gamma_2 \gamma_i) + \cdots + x_n S(\gamma_n \gamma_i) \equiv 0 \pmod{p}$$
$$(i = 1, 2, \cdots, n)$$

erfüllt sind, Kongruenzen, welche, wenn

$$\gamma = x_1 \gamma_1 + x_2 \gamma_2 + \cdots + x_n \gamma_n$$

gesetzt wird, durch die folgenden:

$$S(\gamma \gamma_i) \equiv 0 \pmod{p}$$
$$(i = 1, 2, \cdots, n)$$

ersetzt werden können. Aus den letzteren folgt, wenn sie mit beliebigen rationalen ganzen Zahlen $z_1, z_2, \cdots, z_n$ multipliziert und dann addiert werden, die eine, für jede ganze Zahl

$$\zeta = \gamma_1 z_1 + \gamma_2 z_2 + \cdots + \gamma_n z_n$$

des Körpers erfüllte Kongruenz

$$S(\gamma \zeta) \equiv 0 \pmod{p}.$$

Ist η gleichfalls irgend eine solche Zahl, so wird allgemeiner

$$S(\gamma \zeta + p\eta) \equiv 0 \pmod{p} \tag{95}$$

sein, wo nun die Gesamtheit der Zahlen $\gamma\zeta + p\eta$ den größten gemeinsamen Idealteiler $\mathfrak{j}$ der Ideale $\mathfrak{g}\gamma$ und $\mathfrak{g}p$ ausmacht. Da im Ausdrucke für γ die Koeffizienten x_i nicht sämtlich durch p teilbar sind, gehört γ dem Ideale $\mathfrak{g}p$ nicht an, somit ist $\mathfrak{j}$ ein von $\mathfrak{g}p$ selbst verschiedener Teiler des letzteren Ideals. Ist daher dies Ideal oder die Zahl p aus lauter verschiedenen Primidealfaktoren zusammengesetzt, so gibt es unter den letzteren wenigstens eins, es heiße $\mathfrak{p}$, welches nicht in $\mathfrak{j}$ aufgeht, da sonst $\mathfrak{j}$ durch $\mathfrak{g}p$ teilbar, also mit $\mathfrak{g}p$ identisch wäre. Setzt man demnach $\mathfrak{g}p = \mathfrak{p} \cdot \mathfrak{q}$, so muß $\mathfrak{q}$ durch $\mathfrak{j}$ teilbar, jede seiner Zahlen $\varkappa$ also im Ideale $\mathfrak{j}$ enthalten sein und deshalb wegen (95) für jede solche Zahl $\varkappa$ die Kongruenz

$$S(\varkappa) \equiv 0 \pmod{p} \tag{96}$$

erfüllt sein. Läßt sich also nachweisen, daß aus dieser Folgerung ein Widerspruch entsteht, so muß p durch das Quadrat eines Primideals teilbar sein, und die obige Behauptung wäre erwiesen.

Um zu diesem Nachweis zu gelangen, setzen wir, wie im vorigen Kapitel Nr. 22

$$\mathfrak{p} = \{p, P(\varrho)\},$$

und bemerken nun der Reihe nach folgendes.

Erstens. Wenn wieder mit f der Grad des Primideals $\mathfrak{p}$ bezeichnet wird, so bedeutet $P(x)$ eine (mod. p) irreduktible Funktion, also $P(x) = 0$ eine auch schlechthin irreduktible Gleichung desselben Grades. Eine Wurzel ξ dieser letzteren erzeugt einen Körper $K(\xi; R)$ f^{ten} Grades, mit bezug auf welchen wir die Gesamtheit seiner ganzen Zahlen, die Spuren, Normen, Diskriminanten durch die Zeichen $\mathfrak{g}_1$, S_1, N_1, Δ_1 andeuten wollen. Nun kann mittels der Identität $P(\xi) = 0$ jede Potenz ξ^m mit positivem ganzzahligen Exponenten in die Form

$$\xi^m = c_0^{(m)} \cdot 1 + c_1^{(m)} \cdot \xi + \cdots + c_{f-1}^{(m)} \cdot \xi^{f-1} \tag{97}$$

mit rational ganzzahligen Koeffizienten gebracht werden, eine Beziehung, welche wegen der Irreduktibilität der Gleichung $P(x) = 0$ mit der Identität

$$x^m = c_0^{(m)} \cdot 1 + c_1^{(m)} \cdot x + \cdots + c_{f-1}^{(m)} \cdot x^{m-1} + P(x) \cdot Q(x), \tag{98}$$

in der $Q(x)$ eine ganze, ganzzahlige Funktion bedeutet, völlig gleichbedeutend ist. Aus (97) gewinnt man das ganze System von Gleichungen:

$$\left\{\begin{array}{l} 1 \cdot \xi^m = c_0^{(m)} \cdot 1 + c_1^{(m)} \cdot \xi + \cdots + c_{f-1}^{(m)} \cdot \xi^{f-1} \\ \xi \cdot \xi^m = c_0^{(m+1)} \cdot 1 + c_1^{(m+1)} \cdot \xi + \cdots + c_{f-1}^{(m+1)} \cdot \xi^{f-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \xi^{f-1} \cdot \xi^m = c_0^{(m+f-1)} \cdot 1 + c_1^{(m+f-1)} \cdot \xi + \cdots + c_{f-1}^{(m+f-1)} \cdot \xi^{f-1}, \end{array}\right. \tag{99}$$

aus denen, da $1, \xi, \xi^2, \cdots, \xi^{f-1}$ eine Basis des Körpers $K(\xi; R)$ bilden, nach Kap. 1, Nr. 8 die Formel

$$S_1(\xi^m) = s_m$$

zu erschließen ist, wenn zur Abkürzung

$$s_m = c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{f-1}^{(m+f-1)} \tag{100}$$

gesetzt wird.

Nun ist einerseits

$$\Delta_1(1, \xi, \xi^2, \cdots, \xi^{f-1}) = \begin{vmatrix} S_1(1), & S_1(\xi), & \cdots, & S_1(\xi^{f-1}) \\ S_1(\xi), & S_1(\xi^2), & \cdots, & S_1(\xi^f) \\ \cdot & \cdot & \cdot & \cdot \\ S_1(\xi^{f-1}), & S_1(\xi^f), & \cdots, & S_1(\xi^{2f-2}) \end{vmatrix},$$

einfacher also

$$(101) \quad \Delta_1(1, \xi, \xi^2, \cdots, \xi^{f-1}) = \begin{vmatrix} s_0, & s_1, \cdots, s_{f-1} \\ s_1, & s_2, \cdots, s_f \\ \cdot & \cdot \quad \cdot \quad \cdot \\ s_{f-1}, & s_f, \cdots, s_{2f-2} \end{vmatrix},$$

eine Determinante, welche kurz S genannt werde. Andererseits besteht die Gleichung

$$\Delta_1(1, \xi, \xi^2, \cdots, \xi^{f-1}) = \pm N_1 P'(\xi).$$

Da aber $P(x)$ (mod. p) irreduktibel ist, so ist $P'(x)$ (mod. p) relativ prim zu $P(x)$, es findet also eine Kongruenz statt von der Gestalt

$$P(x)\varphi(x) + P'(x)\psi(x) \equiv 1 \text{ (mod. } p),$$

aus welcher für $x = \xi$ sich $P'(\xi)\psi(\xi) \equiv 1$, also das Ideal $\mathfrak{g}_1 P'(\xi)$ sich als relativ prim gegen p ergibt. Daraus folgt nach den ersten Sätzen in Kap. 6, Nr. 18, daß auch $N_1 P'(\xi)$ prim gegen p ist. So ergibt sich als erster für unsere Betrachtung fundamentaler Punkt der Satz: Die mit S bezeichnete Determinante in Formel (101) geht durch die Primzahl p nicht auf.

Zweitens. Die Zahl ϱ war eine Wurzel der Kongruenz $P(x) \equiv 0$ (mod. $\mathfrak{p}$), aber eine Kongruenz

$$(102) \quad a_0 + a_1\varrho + a_2\varrho^2 + \cdots + a_{f-1}\varrho^{f-1} \equiv 0 \text{ (mod. } \mathfrak{p})$$

also auch (mod. p) unmöglich, wenn nicht sämtliche ihrer Koeffizienten durch p teilbar sind. Da nun nach Voraussetzung p aus lauter verschiedenen Primidealen zusammengesetzt ist, so sind $\mathfrak{p}$, $\mathfrak{q}$ relativ prime Ideale, und daher kann eine ganze Zahl γ des Körpers $K(\mathsf{A}; R)$ so gewählt werden, daß

$$\gamma \equiv 1 \text{ (mod. } \mathfrak{p}), \quad \gamma \equiv 0 \text{ (mod. } \mathfrak{q})$$

und daher

$$(103) \quad \gamma^2 \equiv \gamma \text{ (mod. } p)$$

ist. Demnach sind die Zahlen

$$(104) \quad \varkappa_1 = \gamma \cdot 1, \ \varkappa_2 = \gamma \cdot \varrho, \ \cdots, \ \varkappa_f = \gamma \cdot \varrho^{f-1}$$

f in $\mathfrak{q}$ enthaltene und (mod. p) rational unabhängige Zahlen, denn wegen des über (102) Gesagten kann eine Kongruenz

$$a_0\varkappa_1 + a_1\varkappa_2 + \cdots + a_{f-1}\varkappa_f \equiv 0 \text{ (mod. } p)$$

nur bestehen, wenn ihre sämtlichen Koeffizienten teilbar sind durch p. Mehr als f (mod. p) unabhängige Zahlen kann es aber in $\mathfrak{q}$ nicht geben. Denn, wären darin $f+1$ solche, $\varkappa_1, \varkappa_2, \cdots, \varkappa_{f+1}$ vorhanden, sodaß eine ganzzahlige Kongruenz

$$(105) \qquad a_0\varkappa_1 + a_1\varkappa_2 + \cdots + a_f\varkappa_{f+1} \equiv 0 \pmod{p}$$

nicht anders stattfinden könnte, als wenn alle a_i durch p teilbar wären, so könnte diese Kongruenz auch (mod. $\mathfrak{p}$) nur unter derselben Bedingung bestehen, da, wenn sie (mod. $\mathfrak{p}$) stattfände, sie auch (mod. p) erfüllt wäre, indem der lineare Ausdruck (105) auch in $\mathfrak{q}$ enthalten ist. Wenn also $f+1$ (mod. p) unabhängige Zahlen in $\mathfrak{q}$ vorhanden wären, so gäbe es darin auch $f+1$ (mod. $\mathfrak{p}$) unabhängige Zahlen, was nicht sein kann, da es deren sogar in $\mathfrak{g}$ nur f gibt. Demnach sind in $\mathfrak{q}$ genau f (mod. p) unabhängige Zahlen, und hieraus schließt man (Kap. 6, Nr. 18, Schluß), daß für jede Zahl $\varkappa$ in $\mathfrak{q}$ eine ganzzahlige Kongruenz besteht

$$\varkappa \equiv a_0\varkappa_1 + a_1\varkappa_2 + \cdots + a_{f-1}\varkappa_f \pmod{p}.$$

Bezeichnet in gleicher Weise g die genaue Anzahl von in $\mathfrak{p}$ vorhandenen, (mod. p) unabhängigen Zahlen, und sind $\pi_1, \pi_2, \cdots, \pi_g$ solche g Zahlen, so gilt für jede Zahl π in $\mathfrak{p}$ eine ganzzahlige Kongruenz von der Form:

$$\pi \equiv b_1\pi_1 + b_2\pi_2 + \cdots + b_g\pi_g \pmod{p}.$$

Nun sind aber, da $\mathfrak{p}$, $\mathfrak{q}$ relativ prime Ideale sind, auch die $f+g$ Zahlen

$$(106) \qquad \varkappa_1, \varkappa_2, \cdots, \varkappa_f, \pi_1, \pi_2, \cdots, \pi_g$$

(mod. p) unabhängig, nämlich eine ganzzahlige Kongruenz

$$a_0\varkappa_1 + a_1\varkappa_2 + \cdots + a_{f-1}\varkappa_f + b_1\pi_1 + b_2\pi_2 + \cdots + b_g\pi_g \equiv 0 \pmod{p}$$

ist nur möglich, wenn alle a_i, b_i durch p teilbar sind. Denn aus ihr ergäbe sich dieselbe Kongruenz auch (mod. $\mathfrak{p}$) und (mod. $\mathfrak{q}$), von denen die erste, da die π_i in $\mathfrak{p}$ enthalten sind, sich einfacher so schreiben ließe:

$$a_0\varkappa_1 + a_1\varkappa_2 + \cdots + a_{f-1}\varkappa_f \equiv 0 \pmod{\mathfrak{p}},$$

oder, da dieser Ausdruck auch eine in $\mathfrak{q}$ enthaltene Zahl darstellt, auch folgendermaßen:

$$a_0 \varkappa_1 + a_1 \varkappa_2 + \cdots + a_{f-1} \varkappa_f \equiv 0 \pmod{p},$$

eine Kongruenz, welche erfordert, daß alle a_i durch p aufgehen. Aus entsprechenden Gründen nimmt die für (mod. $\mathfrak{q}$) sich ergebende Kongruenz die Form an:

$$b_1 \pi_1 + b_2 \pi_2 + \cdots + b_g \pi_g \equiv 0 \pmod{p},$$

aus der wieder sämtliche b_i als teilbar durch p sich ergäben. Die Behauptung ist also erwiesen.

Da nun $\mathfrak{g} = \mathfrak{p} + \mathfrak{q}$, so besteht für jede ganze Zahl ζ des Körpers $K(\mathsf{A};\, R)$ eine ganzzahlige Kongruenz

$$\zeta \equiv a_0 \varkappa_1 + \cdots + a_{f-1} \varkappa_f + b_1 \pi_1 + \cdots + b_g \pi_g \pmod{p}$$

und es gibt genau p^{f+g} (mod. p) inkongruente Zahlen in $\mathfrak{g}$. Aber nach der Formel

$$(\mathfrak{g},\, \mathfrak{g}p) = \mathfrak{N}(\mathfrak{g}p) = p^n$$

beträgt diese Anzahl p^n, man schließt also die Gleichung

$$f + g = n$$

und hat in den Zahlen (106) n (mod. p) unabhängige Zahlen in $\mathfrak{g}$. Heißt C die Determinante der n linearen Gleichungen, durch welche dieselben mittels der Basiszahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ von $\mathfrak{g}$ ausdrückbar sind, so kann jedes Produkt $C \cdot \gamma_i$ als eine lineare ganzzahlige Funktion der Zahlen (106), und somit auch überhaupt das C-fache jeder ganzen Zahl ζ des Körpers in der Form

$$C \cdot \zeta = a_0 \varkappa_1 + \cdots + a_{f-1} \varkappa_f + b_1 \pi_1 + \cdots + b_g \pi_g \tag{107}$$

dargestellt werden. Wegen der rationalen Unabhängigkeit der Zahlen (106) in bezug auf p kann aber die Determinante C nicht durch p teilbar sein.

Drittens. Nun folgt aus (98) für $x = \varrho$ und indem man mit γ multipliziert, die Kongruenz

$$\gamma \varrho^m \equiv c_0^{(m)} \cdot \varkappa_1 + c_1^{(m)} \cdot \varkappa_2 + \cdots + c_{f-1}^{(m)} \cdot \varkappa_f \pmod{\mathfrak{p}}$$

und, da beide Seiten derselben im Ideale $\mathfrak{q}$ enthalten also auch (mod. $\mathfrak{q}$) kongruent sind, dieselbe Kongruenz auch (mod. p), woraus, wenn man beachtet, daß wegen (103) und (104)

$$\varkappa_i \cdot \gamma \varrho^m \equiv \gamma \cdot \varrho^{m+i-1} \pmod{p}$$

ist, nachfolgendes System von Kongruenzen:

$$(108)\quad \begin{aligned} \varkappa_1 \cdot \gamma\varrho^m &\equiv c_0^{(m)} \cdot \varkappa_1 + c_1^{(m)} \cdot \varkappa_2 + \cdots + c_{f-1}^{m} \cdot \varkappa_f \\ \varkappa_2 \cdot \gamma\varrho^m &\equiv c_0^{(m+1)} \cdot \varkappa_1 + c_1^{(m+1)} \cdot \varkappa_2 + \cdots + c_{f-1}^{(m+1)} \cdot \varkappa_f \quad (\text{mod. } p) \\ &\cdots\cdots\cdots\cdots \\ \varkappa_f \cdot \gamma\varrho^m &\equiv c_0^{(m+f-1)} \cdot \varkappa_1 + c_1^{(m+f-1)} \cdot \varkappa_2 + \cdots + c_{f-1}^{(m+f-1)} \cdot \varkappa_f \end{aligned}$$

hervorgeht. Bedenkt man, daß jede der Zahlen π_i in $\mathfrak{p}$, die Zahl $\gamma\varrho^m$ aber in $\mathfrak{q}$, folglich jedes der Produkte $\pi_i\gamma\varrho^m$ in $\mathfrak{g}p = \mathfrak{p}\mathfrak{q}$ enthalten ist, so darf man dem vorigen Systeme noch das weitere hinzufügen:

$$(108)\quad \pi_1 \cdot \gamma\varrho^m \equiv 0,\ \pi_2 \cdot \gamma\varrho^m \equiv 0, \cdots,\ \pi_g \cdot \gamma\varrho^m \equiv 0 \quad (\text{mod. } p).$$

Werden diese n Kongruenzen (108) aber als Gleichungen geschrieben, indem jeder rechten Seite ein passendes Vielfache von p, d. i. ein Ausdruck von der Form $p \cdot \zeta$ hinzugefügt wird, dessen C-faches wegen (107) gleich

$$p(a_0\varkappa_1 + \cdots + a_{f-1}\varkappa_f + b_1\pi_1 + \cdots + b_g\pi_g)$$

gesetzt werden kann, so lassen die Kongruenzen (108) erkennen, daß die Produkte

$$\varkappa_1 \cdot C\gamma\varrho^m, \cdots, \varkappa_f \cdot C\gamma\varrho^m, \pi_1 \cdot C\gamma\varrho^m, \cdots, \pi_g \cdot C\gamma\varrho^m$$

gleich linearen Funktionen der n (mod. p), also um so mehr auch schlechthin unabhängigen Zahlen (106) sind, deren Koeffizienten von den C-fachen Koeffizienten jener Kongruenzen nur um Vielfache von p sich unterscheiden. Nach Kap. 1, Nr. 8 ist aber die Spur

$$S(C\gamma\varrho^m) = C \cdot S(\gamma\varrho^m)$$

gleich der Summe der in der Diagonale des Koeffizientensystems jener linearen Funktionen stehenden Glieder und folglich (mod. p) kongruent mit der Summe

$$C \cdot [c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{f-1}^{(m+f-1)}],$$

in Rücksicht auf die Formel (100) also

$$C \cdot S(\gamma\varrho^m) \equiv C \cdot s_m \quad (\text{mod. } p).$$

Da jedoch $\gamma\varrho^m$ eine Zahl in $\mathfrak{q}$ ist, schließt man wegen (96) und da C durch p nicht teilbar ist, nachstehende Kongruenz:

$$s_m \equiv 0 \pmod{p},$$

und somit auch, daß die mit S bezeichnete Determinante durch p teilbar ist, gegen das an erster Stelle Bewiesene.

Dieser Widerspruch zeigt die Richtigkeit der behaupteten Umkehrung und folglich ist der letzte Satz der vorigen Nummer über die Primfaktoren der Grundzahl vollständig bewiesen.

15. Dedekind hat sich aber mit diesem Satze über die Grundzahl nicht begnügt, sondern durch eine weitere Untersuchung Resultate gewonnen, die eine viel tiefer dringende Einsicht in die Natur jener wichtigen Zahl gewähren. Die Mitteilung seiner bezüglichen Arbeit[1]) hat mit einer Vorbetrachtung zu beginnen, auf der als der wesentlichen Grundlage dann das übrige leicht sich erbaut.

Sei wieder θ eine beliebige der den Körper erzeugenden ganzen Zahlen und

$$F(x) = 0 \tag{109}$$

die irreduktible Gleichung n^{ten} Grades, durch welche sie bestimmt ist. Jede ganze, ganzzahlige Funktion $\mathfrak{f}(\theta)$ läßt sich auf die Form bringen:

$$\mathfrak{f}(\theta) = c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1}, \tag{110}$$

in der die c_i rationale ganze Zahlen sind, ihre Gesamtheit ist also identisch mit dem Modulus

$$\mathfrak{o} = [1, \theta, \theta^2, \cdots, \theta^{n-1}]. \tag{111}$$

Da das Produkt zweier Ausdrücke von der Form (110) mittels der Identität

$$F(\theta) = 0$$

wieder auf die gleiche Form gebracht werden kann, also ebenfalls im Modulus $\mathfrak{o}$ enthalten ist, so findet die Beziehung statt

$$\mathfrak{o} \cdot \mathfrak{o} = \mathfrak{o},$$

d. h. der Modulus $\mathfrak{o}$ ist eine „Ordnung in $\mathfrak{g}$“. Den Führer dieser Ordnung, der bekanntlich ein Ideal des Körpers ist (s. Kap. 4, Nr. 6), nennen wir $\mathfrak{f}$, sodaß

$$\mathfrak{f} = \frac{\mathfrak{o}}{\mathfrak{g}}.$$

1) Dedekind, über die Diskriminanten endlicher Körper, § 7—14, Götting. Abh. Bd. 29.

Dies vorausgeschickt, sei $\mathfrak{p}$ ein beliebiges Primideal des Körpers, p die darin enthaltene rationale Primzahl, f sein Grad und $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$, sodaß

$$\mathfrak{g}p = \mathfrak{p}^e \cdot \mathfrak{q} \tag{112}$$

gesetzt werden kann und $\mathfrak{q}$ nicht mehr teilbar ist durch $\mathfrak{p}$. Man denke $F(x)$ in seine (mod. p) irreduktibeln Faktoren zerlegt. Da das Produkt der letzteren für $x = \theta$ durch p aufgeht, muß einer der irreduktibeln Faktoren durch $\mathfrak{p}$ teilbar sein. Sei dies der Faktor $P(x)$, m sein Grad, und er gehe ε mal in $F(x)$ auf, sodaß

$$F(x) \equiv P(x)^\varepsilon \cdot \Pi(x) \quad (\text{mod. } p) \tag{113}$$

geschrieben werden kann, während $\Pi(x)$ (mod. p) nicht mehr durch $P(x)$ teilbar ist. Nach Kap. 6, Nr. 21 ist jede Zahl in $\mathfrak{o}$, d. h. jeder Ausdruck $\mathfrak{f}(\theta)$ von der Gestalt (110) einem und auch nur einem Ausdrucke

$$\varphi(\theta) = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{m-1}\theta^{m-1}, \tag{114}$$

in welchem die a_i ganze Zahlen der Reihe $0, 1, 2, \cdots, p-1$ bedeuten, (mod. $\mathfrak{p}$) kongruent und daher die Anzahl der (mod. $\mathfrak{p}$) inkongruenten Zahlen in $\mathfrak{o}$

$$(\mathfrak{o}, \mathfrak{p}) = p^m. \tag{115}$$

Hier gilt nun der folgende Satz, der die Grundlage des Weiteren bildet:

Die erforderlichen und hinreichenden Bedingungen dafür, daß das Ideal $\mathfrak{f}$ nicht durch $\mathfrak{p}$ teilbar sei, bestehen darin, daß $m = f$ und daß $\mathfrak{p}$ der größte gemeinsame Teiler der beiden Hauptideale $\mathfrak{g}p$ und $\mathfrak{g}P(\theta)$ sei, in Zeichen:

$$\mathfrak{p} = \{p, P(\theta)\}.$$

I. Daß diese zwei Bedingungen notwendig sind, erkennt man folgendermaßen. Da (nach Kap. 4, vorletzte Nummer) der Führer $\mathfrak{f}$ in der Ordnung $\mathfrak{o}$ enthalten oder

$$\mathfrak{f} \succ \mathfrak{o}$$

ist, da ferner $\mathfrak{f}$, wenn es nicht durch $\mathfrak{p}$ teilbar ist, prim zu $\mathfrak{p}$ also

$$\mathfrak{f} + \mathfrak{p} = \mathfrak{g}$$

sein muß, so folgt

$$\mathfrak{g} = \mathfrak{f} + \mathfrak{p} \succ \mathfrak{o} + \mathfrak{p} \succ \mathfrak{g}$$

mithin $\mathfrak{g} = \mathfrak{o} + \mathfrak{p}$; daher nimmt die Beziehung

$$(\mathfrak{o}, \mathfrak{p}) = (\mathfrak{o} + \mathfrak{p}, \mathfrak{p})$$

die Form

$$(\mathfrak{o}, \mathfrak{p}) = (\mathfrak{g}, \mathfrak{p}) = \mathfrak{N}(\mathfrak{p}) = p^f$$

an, und ihre Vergleichung mit (115) lehrt, daß **erstens** $m = f$ sein muß.

Ferner sieht man zunächst, daß $\mathfrak{p}$ **gemeinsamer Teiler** von $\mathfrak{g}p$ und $\mathfrak{g}P(\theta)$ ist, da $P(\theta) \equiv 0 \pmod{\mathfrak{p}}$. Wenn aber $\mathfrak{f}$ nicht durch $\mathfrak{p}$, also $\mathfrak{f}\mathfrak{p}$ nicht durch $\mathfrak{p}^2$ teilbar ist, so gibt es in $\mathfrak{f}\mathfrak{p}$ eine durch $\mathfrak{p}$ aber nicht durch $\mathfrak{p}^2$ teilbare Zahl, welche, da $\mathfrak{f}\mathfrak{p} \succ \mathfrak{f} \succ \mathfrak{o}$ ist, die Gestalt $\mathfrak{f}(\theta)$ haben wird. Da nun die Kongruenz

$$\mathfrak{f}(\theta) \equiv 0 \pmod{\mathfrak{p}} \tag{116}$$

nach Kap. 6, Nr. 22 mit der Funktionenkongruenz

$$\mathfrak{f}(x) \equiv P(x)\, Q(x) \pmod{p}, \tag{117}$$

in welcher $Q(x)$ eine ganze, ganzzahlige Funktion von x bezeichnet, gleichbedeutend ist, aus welcher wieder

$$\mathfrak{f}(\theta) \equiv P(\theta)\, Q(\theta) \pmod{p}$$

hervorgeht, so können $P(\theta)$ und p nicht zugleich durch $\mathfrak{p}^2$ teilbar sein. Ist andererseits $\mathfrak{p}'$ ein Primidealfaktor von $\mathfrak{q}$, so gibt es im Ideale $\mathfrak{f}\mathfrak{p}'$, welches nicht durch $\mathfrak{p}$ teilbar, d. i. nicht in $\mathfrak{p}$ enthalten ist, eine nicht zu $\mathfrak{p}$ gehörige, aber wegen $\mathfrak{f}\mathfrak{p}' \succ \mathfrak{f} \succ \mathfrak{o}$ in $\mathfrak{o}$ enthaltene Zahl, also von der Gestalt $\mathfrak{f}(\theta)$; da jetzt aber die Kongruenz (116) nicht statt hat, kann auch (117) nicht statt haben, sondern $P(x)$, $\mathfrak{f}(x)$ müssen $\pmod{p}$ relativ prim sein, also eine Kongruenz bestehen von der Form

$$P(x)\, \psi(x) + \mathfrak{f}(x)\, \chi(x) \equiv 1 \pmod{p},$$

aus der, da nach Voraussetzung $\mathfrak{f}(\theta) \equiv 0 \pmod{\mathfrak{p}'}$ ist, für $x = \theta$ sich

$$P(\theta)\, \psi(\theta) \equiv 1 \pmod{\mathfrak{p}'}$$

ergibt; ihr zufolge kann $P(\theta)$ durch $\mathfrak{p}'$ nicht teilbar sein. Aus

diesen Punkten aber ergibt sich zweitens $\mathfrak{p}$ als größter gemeinsamer Teiler von $\mathfrak{g}p$ und $\mathfrak{g}P(\theta)$ oder

$$\mathfrak{p} = \{p,\ P(\theta)\}, \tag{118}$$

wie zu beweisen war.

II. Die genannten zwei Bedingungen sind aber auch hinreichend. In der Tat, sind sie erfüllt, so ist $P(x)$ eine Primfunktion (mod. p) von gleichem Grade wie das Primideal $\mathfrak{p}$ und θ eine Wurzel der Kongruenz

$$P(x) \equiv 0 \pmod{\mathfrak{p}},$$

welche wegen der zweiten Voraussetzung, wenn zunächst $e > 1$ angenommen wird, völlig die charakteristischen Eigenschaften der in Kap. 6, Nr 22 mit ϱ bezeichneten Zahl besitzt, insbesondere die Eigenschaft, daß $P(\theta)$ zwar durch $\mathfrak{p}$, aber nicht mehr durch $\mathfrak{p}^2$ teilbar ist; demnach ist jede ganze Zahl γ des Körpers einer ganzen, ganzzahligen Funktion von θ, d. i. einer Zahl in $\mathfrak{o}$ (mod. $\mathfrak{p}^e$) kongruent. Diese Folgerung besteht aber auch, wenn $e = 1$ ist, da dann nach derselben Stelle für jede Zahl γ in $\mathfrak{g}$ eine Kongruenz besteht von der Form:

$$\gamma \equiv a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{f-1}\theta^{f-1} \pmod{\mathfrak{p}}.$$

Man darf demzufolge, unter ω eine Zahl in $\mathfrak{o}$ verstehend, immer

$$\gamma \equiv \omega \pmod{\mathfrak{p}^e} \tag{119}$$

setzen. Nun folgt für $x = \theta$ aus (113)

$$P(\theta)^e \cdot \Pi(\theta) \equiv 0 \pmod{p}$$

also auch (mod. $\mathfrak{q}$), und da $P(\theta)$ wegen der vorausgesetzten Gleichung (118) relativ prim zu $\mathfrak{q}$ ist, $\Pi(\theta)$ teilbar durch $\mathfrak{q}$, dagegen nicht teilbar durch $\mathfrak{p}$, da $\Pi(x)$ (mod. p) nicht durch $P(x)$ teilbar ist. Da wegen (119) die Zahl $\gamma - \omega$ durch $\mathfrak{p}^e$ aufgeht, so ist $(\gamma - \omega) \cdot \Pi(\theta)$ durch $\mathfrak{p}^e \cdot \mathfrak{q}$, d. i. durch p teilbar, sodaß

$$\gamma \cdot \Pi(\theta) = \omega \cdot \Pi(\theta) + p \cdot \gamma_1$$

gesetzt werden darf, wo auch γ_1 eine ganze Zahl des Körpers bedeutet. In dieser Gleichung sind aber ω, $\Pi(\theta)$ zwei zur Ordnung $\mathfrak{o}$ gehörige Zahlen, der somit auch ihr Produkt angehört, sodaß die Gleichung als Kongruenz folgendermaßen

geschrieben werden kann:

$$\gamma \cdot \Pi(\theta) \equiv p \cdot \gamma_1 \pmod{\mathfrak{o}}.$$

Da hier γ eine beliebige Zahl in $\mathfrak{g}$ bedeutet, erhält man ebenso der Reihe nach die anderen Kongruenzen:

$$\left.\begin{array}{l} \gamma_1 \quad \cdot \Pi(\theta) \equiv p \cdot \gamma_2 \\ \gamma_2 \quad \cdot \Pi(\theta) \equiv p \cdot \gamma_3 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \gamma_{s-1} \cdot \Pi(\theta) \equiv p \cdot \gamma_s \end{array}\right\} \pmod{\mathfrak{o}},$$

welche, weil $\mathfrak{o}$ eine Ordnung ist, mit der zu $\mathfrak{o}$ gehörigen Zahl $\Pi(\theta)$ multipliziert werden können, woraus dann die folgende hervorgeht:

$$\gamma \cdot \Pi(\theta)^s \equiv \gamma_s \cdot p^s \pmod{\mathfrak{o}}.$$

Hier möge unter s der Exponent der höchsten Potenz von p verstanden werden, welche im Index C der Zahl θ aufgeht, sodaß $C = cp^s$ gesetzt werden kann, während c durch p nicht teilbar ist. Wählt man $k = c \cdot \Pi(\theta)^s$, so liefert die letzte Kongruenz die Beziehung

$$\gamma k \equiv C \cdot \gamma_s \pmod{\mathfrak{o}}.$$

Nun bedeutet aber der Index C von θ die Determinante der n linearen Gleichungen, durch welche die Potenzen $1, \theta, \theta^2, \cdots, \theta^{n-1}$ mittels der Basiszahlen von $\mathfrak{g}$ ausdrückbar sind; die C-fachen Basiszahlen, mithin allgemeiner das C-fache jeder Zahl in $\mathfrak{g}$ werden also umgekehrt durch jene Potenzen ausdrückbar, nämlich in $\mathfrak{o}$ enthalten sein. Die Kongruenz lehrt also einfacher, daß jedes Vielfache von k, oder daß das gesamte Ideal $\mathfrak{g}k$ in $\mathfrak{o}$ enthalten ist. Nach Kap. 4, vorletzte Nummer ist aber jedes in der Ordnung $\mathfrak{o}$ enthaltene Ideal teilbar durch ihren Führer $\mathfrak{f}$. Wäre letzterer teilbar durch $\mathfrak{p}$, so müßte also auch $\mathfrak{g}k$ durch $\mathfrak{p}$ teilbar sein, während doch die Zahl k selbst diesen Primidealteiler nicht enthält. Hieraus folgt, daß $\mathfrak{f}$ nicht durch $\mathfrak{p}$ teilbar sein kann, w. z. b. w.

An den so bewiesenen Satz schließen wir sogleich den anderen an:

Für jedes gegebene Primideal $\mathfrak{p}$ *gibt* es stets eine den Körper erzeugende ganze Zahl θ von der Beschaffenheit, daß $\mathfrak{p}$ im Führer $\mathfrak{f}$ ihrer Ordnung $\mathfrak{o}$ nicht

aufgeht. Zum Beweise sei ϱ eine Zahl, wie sie im Kap. 6, Nr. 22 nachgewiesen worden ist, für welche

$$\mathfrak{p} = \{p,\ P(\varrho)\}$$

ist. Ferner sei ζ eine beliebig gewählte, den Körper erzeugende ganze Zahl, $\mathrm{F}(x) = 0$ die irreduktible Gleichung der sie genügt; die Differente

$$(120) \qquad \partial(\zeta) = \mathrm{F}'(\zeta) = (\zeta - \zeta^{(1)})(\zeta - \zeta^{(2)}) \cdots (\zeta - \zeta^{(n-1)}),$$

wo $\zeta^{(1)}, \zeta^{(2)}, \cdots, \zeta^{(n-1)}$ die zu ζ konjugierten Zahlen bezeichnen, ist dann (Kap. 1, Nr. 14) von Null verschieden. Setzt man nun, unter x eine beliebige rationale ganze Zahl verstehend,

$$(121) \qquad \theta = \varrho + px\zeta,$$

so wird θ eine ganze Zahl des Körpers und $P(\theta) \equiv P(\varrho)$ (mod. p), demnach

$$\mathfrak{p} = \{p,\ P(\theta)\}.$$

Die Funktion $P(x)$ bedeutet aber eine Primfunktion f^{ten} Grades (mod. $\mathfrak{p}$) und ϱ eine Wurzel der Kongruenz

$$P(x) \equiv 0 \pmod{\mathfrak{p}}.$$

Hieraus folgt wegen (121) auch $P(\theta) \equiv 0$ (mod. $\mathfrak{p}$), und, wenn $F(x) = 0$ die Gleichung n^{ten} Grades ist, welcher die Zahl θ des Körpers genügt, so muß, da $F(\theta) = 0$, also auch $\equiv 0$ (mod. $\mathfrak{p}$) ist, $F(x)$ (mod. p) durch $P(x)$ teilbar, also $P(x)$ ein (mod. p) irreduktibler Faktor von $F(x)$ sein. Aus alle diesem ersieht man, daß es eine solche Zahl θ gibt, für welche die Bedingungen des vorigen Satzes zutreffen, und daß daher $\mathfrak{p}$ im Führer $\mathfrak{f}$ der dieser Zahl entsprechenden Ordnung $\mathfrak{o}$ nicht aufgeht. Nach (121) folgt nämlich für jeden der Indizes $i = 1, 2, \cdots, n-1$

$$\theta - \theta^{(i)} = \varrho - \varrho^{(i)} + px(\zeta - \zeta^{(i)});$$

da nun wegen (120) keine der Differenzen $\zeta - \zeta^{(i)}$ Null ist, weil es $\partial(\zeta)$ nicht ist, so kann die rationale ganze Zahl x jedenfalls so gewählt werden, daß auch keine der Differenzen $\theta - \theta^{(i)}$ verschwindet, mithin die Differente $\partial(\theta)$ von Null verschieden, d. h. die Gleichung $F(x) = 0$ irreduktibel, θ also eine erzeugende ganze Zahl des Körpers wird. Somit ist der behauptete Satz bewiesen.

Es verdient bemerkt zu werden, daß, während nach dem, was in Nr. 10 und 11 festgestellt ist, bisweilen der Fall sich ereignet, daß eine Primzahl p ein Teiler der Indizes sämtlicher Zahlen der Gattung $\mathfrak{G}$ ist, dem eben bewiesenen Satze zufolge es niemals geschieht, daß ein Primideal $\mathfrak{p}$ in sämtlichen, ihnen entsprechenden Führern aufgeht.

16. Nach dieser Voruntersuchung knüpfen wir an Verhältnisse wieder an, welche in Kap. 1, Nr. 16 entwickelt worden sind.

Bildeten $\omega_1, \omega_2, \cdots, \omega_n$ eine Basis des Körpers, welche hier stets als aus ganzen Zahlen bestehend gedacht werde, so hieß $\omega_1', \omega_2', \cdots, \omega_n'$ eine zu jener komplementäre Basis wenn die Gleichungen

$$\omega_i = \sum_{k=1}^{n} S(\omega_i \omega_k) \cdot \omega_k' \qquad (i = 1, 2, \cdots, n) \tag{122}$$

erfüllt waren. Ist nun $\mathfrak{a}$ irgend ein (aus ganzen Zahlen bestehender) n-gliedriger Modulus, dessen Basiszahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$ also auch eine Basis des Körpers bilden, so bestimmen die Elemente $\alpha_1', \alpha_2', \cdots, \alpha_n'$ der komplementären Basis ebenfalls einen im Körper enthaltenen Modulus, welcher von der willkürlichen Wahl der Basis des Modulus $\mathfrak{a}$ unabhängig ist und der zu $\mathfrak{a}$ komplementäre Modulus heißen mag. Daß in der Tat die besondere Wahl der Basis von $\mathfrak{a}$ ohne Einfluß ist, ergibt sich aus der Bemerkung, daß, wenn $\beta_1, \beta_2, \cdots, \beta_n$ irgend eine andere Basis des Modulus $\mathfrak{a}$ also auch des Körpers bedeuten, welche mit der ersteren durch n lineare Gleichungen

$$\beta_i = \varrho_{i1}\alpha_1 + \varrho_{i2}\alpha_2 + \cdots + \varrho_{in}\alpha_n \qquad (i = 1, 2, \cdots, n)$$

mit der Determinante ± 1 verbunden ist, nach den a. a. O. abgeleiteten Sätzen zwischen den komplementären Basen die Gleichungen

$$\alpha_i' = \varrho_{1i}\beta_1' + \varrho_{2i}\beta_2' + \cdots + \varrho_{ni}\beta_n' \qquad (i = 1, 2, \cdots, n)$$

bestehen, welche lehren, daß sie zwei Basen eines und desselben Modulus bilden. Nennt man den zu $\mathfrak{a}$ komplementären

Modulus $\mathfrak{a}'$, so leuchtet aus der Tatsache, daß die Basis $\alpha_1, \alpha_2, \cdots, \alpha_n$ wieder die komplementäre zur Basis $\alpha_1', \alpha_2', \cdots, \alpha_n'$ ist, sogleich ein, daß $\mathfrak{a}$ der zu $\mathfrak{a}'$ komplementäre Modulus ist, was durch die Gleichung

$$(123) \qquad (\mathfrak{a}')' = \mathfrak{a}$$

ausgedrückt werden soll.

Hier gelten nun einige einfach zu beweisende Sätze.

1) Sind $\mathfrak{a}$, $\mathfrak{b}$ zwei n-gliedrige Moduln ganzer Zahlen, und ferner $\mathfrak{a} \succ \mathfrak{b}$, so ist $\mathfrak{b}' \succ \mathfrak{a}'$ und $(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', \mathfrak{b}')$. In der Tat, wenn $\alpha_1, \alpha_2, \cdots, \alpha_n$; $\beta_1, \beta_2, \cdots, \beta_n$ die Basen der Moduln $\mathfrak{a}$, $\mathfrak{b}$ resp. bezeichnen, so folgen aus der Annahme n ganzzahlige Gleichungen

$$\alpha_i = \varrho_{i1}\beta_1 + \varrho_{i2}\beta_2 + \cdots + \varrho_{in}\beta_n, \quad (i = 1, 2, \cdots, n)$$

aus denen die folgenden:

$$\beta_i' = \varrho_{1i}\alpha_1' + \varrho_{2i}\alpha_2' + \cdots + \varrho_{ni}\alpha_n' \quad (i = 1, 2, \cdots, n)$$

hervorgehen, welche zeigen, daß $\mathfrak{b}' \succ \mathfrak{a}'$. Da zudem die Determinante der ersteren Gleichungen nach Schluß des 2. Kapitels die Zahl $(\mathfrak{b}, \mathfrak{a})$, die ihr gleiche Determinante der letzteren Gleichungen ebenso die Zahl $(\mathfrak{a}', \mathfrak{b}')$ bestimmt, so sind auch diese beiden Anzahlen einander gleich.

2) Desgleichen ist für zwei solche Moduln $\mathfrak{a}$, $\mathfrak{b}$ stets

$$(\mathfrak{a} + \mathfrak{b})' = \mathfrak{a}' - \mathfrak{b}'.$$

Denn, da $\mathfrak{a}$, $\mathfrak{b}$ in $\mathfrak{a} + \mathfrak{b}$ enthalten sind, so ist dem eben Bewiesenen zufolge $(\mathfrak{a} + \mathfrak{b})'$ sowohl in $\mathfrak{a}'$ als auch in $\mathfrak{b}'$ enthalten, folglich auch in $\mathfrak{a}' - \mathfrak{b}'$; da aber $\mathfrak{a}' - \mathfrak{b}'$ sowohl in $\mathfrak{a}'$ als in $\mathfrak{b}'$ enthalten ist, folgt mit Rücksicht auf (123) sowohl $\mathfrak{a}$ als auch $\mathfrak{b}$ und daher auch $\mathfrak{a} + \mathfrak{b}$ enthalten in $(\mathfrak{a}' - \mathfrak{b}')'$, woraus nach dem vorigen Satze und wieder mit Rücksicht auf (123) umgekehrt auch $\mathfrak{a}' - \mathfrak{b}'$ enthalten in $(\mathfrak{a} + \mathfrak{b})'$ sich ergibt. Aus beiden Resultaten folgt der Satz.

3) Hieraus geht $(\mathfrak{a}\mathfrak{b})' = \frac{\mathfrak{b}'}{\mathfrak{a}}$ hervor. In der Tat, sind $\alpha_1, \alpha_2, \cdots, \alpha_n$ die Basiszahlen von $\mathfrak{a}$, so ist der Modulus $\mathfrak{a}\mathfrak{b}$ der größte gemeinsame Teiler der Moduln

(124) $$\mathfrak{b}\alpha_1,\ \mathfrak{b}\alpha_2,\ \cdots,\ \mathfrak{b}\alpha_n;$$

durch einfache Verallgemeinerung des vorigen Satzes folgt hieraus, daß $(\mathfrak{a}\mathfrak{b})'$ das kleinste gemeinsame Vielfache der n zu den Moduln (124) komplementären Moduln

(125) $$(\mathfrak{b}\alpha_1)',\ (\mathfrak{b}\alpha_2)',\ \cdots,\ (\mathfrak{b}\alpha_n)'$$

ist. Nun besteht nach (85) des ersten Kapitels zwischen den Basiszahlen der komplementären Moduln $\mathfrak{b}$, $\mathfrak{b}'$ die Beziehung

$$S(\beta_i'\beta_k) = (i, k),$$

worin (i, k) gleich 1 oder 0, jenachdem i, k einander gleich oder verschieden sind; setzt man also $\omega_k = \beta_k\alpha_1$, $\omega_i' = \beta_i'\alpha_1^{-1}$, so wird ebenfalls

$$S(\omega_i'\omega_k) = (i, k)$$

sein, was nach der angeführten Stelle aussagt, daß die Moduln mit den Basiszahlen $\beta_k\alpha_1$ resp. $\beta_i'\alpha_1^{-1}$, d. h. die Moduln $\mathfrak{b}\alpha_1$ und $\mathfrak{b}'\alpha_1^{-1}$ komplementäre Moduln sind. Hiernach sind die Moduln (125) mit den folgenden identisch:

$$\mathfrak{b}'\alpha_1^{-1},\ \mathfrak{b}'\alpha_2^{-1},\ \cdots,\ \mathfrak{b}'\alpha_n^{-1},$$

deren kleinstes gemeinsames Vielfache nach Kap. 4, Nr. 6 gleich $\frac{\mathfrak{b}'}{\mathfrak{a}}$ ist. Also ist wirklich $(\mathfrak{a}\mathfrak{b})' = \frac{\mathfrak{b}'}{\mathfrak{a}}$.

Insbesondere folgt hieraus, daß komplementäre Moduln die gleiche Ordnung besitzen. Denn, wählt man $\mathfrak{b} = \mathfrak{a}'$, also $\mathfrak{b}' = (\mathfrak{a}')' = \mathfrak{a}$, so folgt

$$(\mathfrak{a}\mathfrak{a}')' = \frac{\mathfrak{a}}{\mathfrak{a}},$$

wegen der Symmetrie in bezug auf $\mathfrak{a}$ und $\mathfrak{a}'$ aber auch

$$(\mathfrak{a}\mathfrak{a}')' = \frac{\mathfrak{a}'}{\mathfrak{a}'}$$

mithin $\mathfrak{a}^0 = (\mathfrak{a}')^0$.

17. Sei nun wieder θ eine den Körper erzeugende ganze Zahl und

(126) $$F(x) = x^n + c_1x^{n-1} + \cdots + c_n = 0$$

die irreduktible Gleichung n^{ten} Grades, durch welche sie bestimmt wird. Setzt man

(127) $$\frac{F(x)}{x-\theta} = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0,$$

so ergeben sich nach Kap. 6, Nr. 4 für die Koeffizienten a_i nachstehende Werte:

$$\begin{aligned}
a_{n-1} &= 1 \\
a_{n-2} &= \theta + c_1 \\
a_{n-3} &= \theta^2 + c_1\theta + c_2 \\
&\cdots\cdots\cdots \\
a_1 &= \theta^{n-2} + c_1\theta^{n-3} + \cdots + c_{n-2} \\
a_0 &= \theta^{n-1} + c_1\theta^{n-2} + \cdots + c_{n-2}\theta + c_{n-1},
\end{aligned}$$

welche sämtlich der Ordnung $\mathfrak{o}$ angehören, die der Zahl θ entspricht, und, da die Determinante der vorstehenden Gleichungen gleich 1 ist, eine Basis derselben bilden. Wir suchen zunächst zu dieser Ordnung, die ein Modulus von der im vorigen vorausgesetzten Beschaffenheit ist, den komplementären Modulus. Bemerken wir hierzu, daß jede Zahl ζ des Körpers eine ganze Funktion $f(\theta)$ vom $n-1^{\text{ten}}$ Grade ist, daß also nach der Lagrangeschen Interpolationsformel

$$f(x) = \frac{f(\theta)}{F'(\theta)}\cdot\frac{F(x)}{x-\theta} + \frac{f(\theta^{(1)})}{F'(\theta^{(1)})}\cdot\frac{F(x)}{x-\theta^{(1)}} + \cdots + \frac{f(\theta^{(n-1)})}{F'(\theta^{(n-1)})}\cdot\frac{F(x)}{x-\theta^{(n-1)}}$$

ist, wo $\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n-1)}$ die Konjugierten zu θ bedeuten, und daß dieser Gleichung mittels des Spurzeichens S die einfachere Gestalt:

$$f(x) = S\left(\frac{f(\theta)}{F'(\theta)}\cdot\frac{F(x)}{x-\theta}\right)$$

gegeben werden kann. Durch Substitution des Ausdrucks (127) geht sie in die folgende über:

$$f(x) = \sum_{i=0}^{n-1} S\left(\frac{f(\theta)}{F'(\theta)}\cdot a_i\right)\cdot x^i,$$

aus dieser aber geht für $x = \theta$ diese andere:

$$\zeta = \sum_{i=0}^{n-1} S\left(\frac{a_i\zeta}{\partial}\right)\cdot\theta^i$$

hervor, in welcher ∂ die Differente $\partial(\theta) = F'(\theta)$ bedeutet. Vergleicht man diese, für jede Zahl ζ des Körpers gefundene Beziehung zwischen den Zahlen

$$(128) \qquad 1,\ \theta,\ \theta^2,\ \cdots,\ \theta^{n-1}$$

einerseits und den Zahlen

$$(129)\qquad \frac{a_0}{\partial},\ \frac{a_1}{\partial},\ \cdots,\ \frac{a_{n-1}}{\partial}$$

andererseits mit der Formel (84) des ersten Kapitels, so leuchtet aus den dort an diese geknüpften Betrachtungen ein, daß die Zahlen (129) das Komplement zu den Zahlen (128) bilden, oder daß der Modulus

$$\left[\frac{a_0}{\partial},\ \frac{a_1}{\partial},\ \cdots,\ \frac{a_{n-1}}{\partial}\right]$$

gleich $\mathfrak{o}'$, also

$$[a_0,\ a_1,\ \cdots,\ a_{n-1}] = \partial\cdot\mathfrak{o}'$$

ist. Da, wie zuvor bemerkt, die Elemente des links stehenden Modulus eine Basis von $\mathfrak{o}$ bilden, ist er nichts anderes als $\mathfrak{o}$, und somit ergibt sich

$$\mathfrak{o} = \partial\cdot\mathfrak{o}',$$

aus welcher Gleichung durch Multiplikation mit $\mathfrak{g}$ in anbetracht der Beziehung $\mathfrak{g}\mathfrak{o} = \mathfrak{g}$ (Kap. 4, (41)) die folgende:

$$(130)\qquad \mathfrak{g} = \partial\cdot\mathfrak{g}\mathfrak{o}'$$

also (nach 3) voriger Nummer)

$$\partial\cdot\mathfrak{g}' = (\mathfrak{g}\mathfrak{o}')'$$

sich findet. Da nun (nach derselben Stelle) $(\mathfrak{g}\mathfrak{o}')' = \frac{\mathfrak{o}}{\mathfrak{g}}$, d. i. gleich dem Führer $\mathfrak{f}$ der Ordnung $\mathfrak{o}$ gesetzt werden darf, so erhält man nachstehende wichtige Gleichung:

$$(131)\qquad \mathfrak{f} = \partial\cdot\mathfrak{g}'.$$

Andererseits besteht zwischen den Basiszahlen γ_i von $\mathfrak{g}$ und den Basiszahlen γ_k' des komplementären Modulus $\mathfrak{g}'$ die Beziehung

$$(132)\qquad \gamma_i = \sum_{k=1}^{n} S(\gamma_i\gamma_k)\cdot\gamma_k',$$

woraus, da die Spuren $S(\gamma_i\gamma_k)$ rationale ganze Zahlen sind, folgt, daß

$$(133)\qquad \mathfrak{g} \succ \mathfrak{g}'$$

sowie (vgl. Schluß von Kap. 2), daß die Determinante $|S(\gamma_i\gamma_k)|$, d. i. die Grundzahl D des Körpers nach ihrem Absolutwerte

die Anzahl $(\mathfrak{g}', \mathfrak{g})$ der Klassen ist, in welche die Zahlen in $\mathfrak{g}'$ sich (mod. $\mathfrak{g}$) verteilen, in Zeichen:

$$\pm D = (\mathfrak{g}', \mathfrak{g}) = (D\mathfrak{g}', D\mathfrak{g}). \tag{134}$$

Da durch Auflösung der Gleichungen (132) jedes Produkt $D\gamma_k'$, mithin auch das D-fache jeder in $\mathfrak{g}'$ enthaltenen Zahl als eine Zahl in $\mathfrak{g}$ sich ergibt, so ist

$$D \cdot \mathfrak{g}' \succ \mathfrak{g}.$$

Der Modulus $D \cdot \mathfrak{g}'$ aber ist ein Ideal, denn, da die Ordnung von $\mathfrak{g}'$ nach der Schlußbemerkung in 3) voriger Nummer gleich der Ordnung von $\mathfrak{g}$, d. h. gleich $\mathfrak{g}$, also $\mathfrak{g}\mathfrak{g}' = \mathfrak{g}'$ ist, muß

$$\mathfrak{g} \cdot (D\mathfrak{g}') = D \cdot (\mathfrak{g}\mathfrak{g}') = D\mathfrak{g}'$$

sein, was die Behauptung bestätigt. Da nun wegen (133) $D \cdot \mathfrak{g} \succ D \cdot \mathfrak{g}'$, d. h. das erstere Ideal durch das zweite Ideal teilbar ist, so kann gesetzt werden:

$$D\mathfrak{g} = D\mathfrak{g}' \cdot \mathfrak{d},$$

wo auch $\mathfrak{d}$ ein Ideal bedeutet.

Dies auf solche Weise oder durch die einfachere Gleichung

$$\mathfrak{g} = \mathfrak{g}' \cdot \mathfrak{d} \tag{135}$$

definierte Ideal ist von hervorragender Bedeutung und soll deshalb *das Grundideal des Körpers* genannt werden. Mit der Grundzahl desselben ist es durch die einfache Tatsache verknüpft, daß die Grund*zahl* absolut genommen die *Norm* des Grund*ideales* ist. In der Tat folgt aus (134)

$$\pm D = (D\mathfrak{g}', \mathfrak{d} \cdot D\mathfrak{g}'),$$

woraus nach Formel (111ᵃ) des 6. Kapitels die andere Gleichung

$$\pm D = (\mathfrak{g}, \mathfrak{d}) = \mathfrak{N}(\mathfrak{d})$$

hervorgeht.

Multipliziert man nun die Gleichung (131) mit $\mathfrak{d}$, so kommt mit Beachtung der das Grundideal definierenden Gleichung (135)

$$\mathfrak{d} \cdot \mathfrak{f} = \mathfrak{g}\varepsilon. \tag{136}$$

Diese Gleichung lehrt, daß das Grundideal $\mathfrak{d}$ ein gemeinsamer, genauer: der *größte* gemeinsame Teiler der Differenten sämtlicher Zahlen θ der Gattung $\mathfrak{G}$

ist; denn hätten diese Differenten einen noch größeren Teiler gemeinsam, so müßten die sämtlichen, den Ordnungen der Zahlen θ entsprechenden Führer $\mathfrak{f}$ noch durch ein gemeinsames Primideal $\mathfrak{p}$ teilbar sein, während doch, wie letzteres auch gewählt werde, nach Nr. 15 eine Zahl θ der Gattung vorhanden ist, in deren Führer $\mathfrak{f}$ es nicht aufgeht.

18. Hiernach ist die Kenntnis des Grundideals und seiner Zusammensetzung aus Primidealen von eminenter Wichtigkeit. Falls im Körper eine Zahl θ vorhanden ist, deren Potenzen $1, \theta, \theta^2, \cdots, \theta^{n-1}$ eine Basis von $\mathfrak{g}$ ausmachen oder deren Ordnung $\mathfrak{o}$ gleich $\mathfrak{g}$ ist,[1]) läßt es sich unmittelbar aus θ bestimmen; denn alsdann gibt die Gleichung (130), da auch $\mathfrak{o}' = \mathfrak{g}'$ sein muß

$$\mathfrak{g} = \partial \cdot \mathfrak{g}\mathfrak{g}',$$

woraus in Verbindung mit (135) die Gleichung

$$\mathfrak{d} \cdot D\mathfrak{g}' = \mathfrak{g}\partial \cdot D\mathfrak{g}'$$

d. i. diese andere:

$$\mathfrak{d} = \mathfrak{g}\partial = \mathfrak{g}\partial(\theta)$$

hervorgeht, durch welche das Grundideal bestimmt ist. In jedem Falle aber läßt sich seine Zusammensetzung durch folgende Betrachtung ermitteln.

Sei wieder $\mathfrak{p}$ ein beliebiges Primideal und θ eine den Körper erzeugende ganze Zahl, in deren Ordnungsführer $\mathfrak{f}$ das Primideal $\mathfrak{p}$ nicht aufgeht. Dann läßt sich zuvörderst zeigen, daß der Exponent ε in der Formel (113) mit dem Exponenten e in der Formel (112) identisch ist. Denn da nach der ersteren Formel $P(\theta)^\varepsilon \cdot \Pi(\theta)$ durch $\mathfrak{p}^\varepsilon \cdot \mathfrak{q}$, der gemachten Voraussetzung zufolge aber, wie in Nr. 15 bemerkt

---

1) Dies trifft z. B. in jedem quadratischen Körper zu; denn, setzt man in Kap. 5, Nr. 1

$$\theta = \frac{D + \sqrt{D}}{2},$$

so findet sich

$$\theta^2 - D\theta + \frac{D(D-1)}{4} = 0,$$

wo $\frac{D(D-1)}{4}$ immer eine ganze Zahl, θ also eine ganze algebraische Zahl zweiten Grades und $\mathfrak{g}$ mit ihrer Ordnung $[1, \theta]$ identisch ist.

worden, $\Pi(\theta)$ nicht durch $\mathfrak{p}$ und $P(\theta)$ nur durch die erste Potenz von $\mathfrak{p}$ teilbar ist, so muß $P(\theta)^{\varepsilon}$ durch $\mathfrak{p}^{\varepsilon}$ teilbar und $\varepsilon \overline{\gtrless} e$ sein. Weil andererseits $\Pi(\theta)$ durch $\mathfrak{q}$ aufgeht, darf

$$P(\theta)^{\varepsilon} \cdot \Pi(\theta) = p \cdot \gamma$$

gesetzt werden, wo γ eine ganze Zahl des Körpers bedeutet, eine Gleichung, aus welcher durch Multiplikation mit der a. a. O. mit k bezeichneten Zahl und bei Beachtung des Umstandes, daß jedes Vielfache γk in der Ordnung $\mathfrak{o}$ von θ enthalten, also eine ganze, ganzzahlige Funktion $\mathfrak{f}(\theta)$ ist, die folgende entspringt:

$$c \cdot P(\theta)^{\varepsilon} \Pi(\theta)^{\varepsilon+1} = p \cdot \mathfrak{f}(\theta),$$

die ihrerseits wegen der Irreduktibilität der Gleichung $F(x) = 0$ mit der andern:

$$c \cdot P(x)^{\varepsilon} \Pi(x)^{\varepsilon+1} = p \cdot \mathfrak{f}(x) + F(x) \cdot Q(x),$$

in welcher $Q(x)$ eine ganze, ganzzahlige Funktion bezeichnet, gleichbedeutend ist.

Aus dieser folgt nun wieder wegen (113)

$$c \cdot P(x)^{\varepsilon} \cdot \Pi(x)^{\varepsilon+1} \equiv P(x)^{e} \cdot \Pi(x) \cdot Q(x) \pmod{p},$$

was umgekehrt, da c relativ prim gegen p und $\Pi(x)$ (mod. p) relativ prim zu $P(x)$ ist, $e > \varepsilon$ erfordert. Hiernach muß schließlich

$$e = \varepsilon$$

sein, wie behauptet.

Dadurch nimmt die Formel (113) die Gestalt an:

$$F(x) \equiv P(x)^{e} \cdot \Pi(x) \pmod{p},$$

eine Kongruenz, welche mittels Differenzierung zu der folgenden führt:

$$F'(x) \equiv P(x)^{e-1} \cdot \Pi_1(x) \pmod{p}, \tag{137}$$

worin

$$\Pi_1(x) = eP'(x)\Pi(x) + P(x)\Pi'(x)$$

gedacht ist.

Ist nun erstens e nicht teilbar durch p, so ist $\Pi_1(x)$ (mod. p) relativ prim zu $P(x)$, da sowohl $P'(x)$ als $\Pi(x)$ es ist; demnach kann $\Pi_1(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein; da aber zufolge (137) $F'(\theta) \equiv P(\theta)^{e-1} \cdot \Pi_1(\theta)$ (mod. $\mathfrak{p}^{e}$) ist, so wird

in diesem Falle $F'(\theta)$, d. i. ∂ genau durch $\mathfrak{p}^{e-1}$ teilbar sein. — Ist aber zweitens e teilbar durch p, so geht $\Pi_1(x)$ (mod. p) durch $P(x)$ auf, mithin ist $\Pi_1(\theta) \equiv 0$ (mod. $\mathfrak{p}$) und $\partial = F'(\theta)$ geht sicher auf durch $\mathfrak{p}^e$, was nicht ausschließt, daß es auch noch durch eine höhere Potenz von $\mathfrak{p}$ teilbar ist. Beachtet man nun die Gleichung (136) und daß $\mathfrak{f}$ nach der Voraussetzung den Primidealfaktor $\mathfrak{p}$ nicht besitzt, so findet sich der folgende Hauptsatz:

Ist $\mathfrak{p}$ ein beliebiges Primideal und p die ihm entsprechende rationale Primzahl, ferner $\mathfrak{p}^e$ die höchste Potenz von $\mathfrak{p}$, die in ihr aufgeht, so enthält das Grundideal $\mathfrak{d}$ allemal die Potenz $\mathfrak{p}^{e-1}$ und zwar, wenn e nicht teilbar ist durch p, keine höhere Potenz, entgegengesetzten Falls aber mindestens die Potenz $\mathfrak{p}^e$ zum Faktor.

Aus diesem Satze über das Grund*ideal* fließt nun aufs neue der in Nr. 13 hergeleitete Satz über die Zusammensetzung der Grund*zahl*. Denn, da diese die Norm von jenem ist, so kann eine in ihr auftretende Potenz einer rationalen Primzahl p nur herrühren von Primidealen des Grundideals, welche in p aufgehen. Sei also wieder

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r};$$

dem Hauptsatze zufolge gehen dann, wenn keiner der Exponenten e_i durch p teilbar ist, in $\mathfrak{d}$ genau die Potenzen

$$\mathfrak{p}_1^{e_1-1},\ \mathfrak{p}_2^{e_2-1},\ \ldots,\ \mathfrak{p}_r^{e_r-1} \tag{138}$$

auf, die für die Norm die Potenzen

$$p^{f_1(e_1-1)},\ p^{f_2(e_2-1)},\ \ldots,\ p^{f_r(e_r-1)} \tag{139}$$

liefern, und somit geht in diesem Falle die Grundzahl D genau auf durch

$$p^{f_1(e_1-1)+f_2(e_2-1)+\cdots+f_r(e_r-1)}. \tag{140}$$

Ist aber mindestens einer der Exponenten e_i teilbar durch p, so geht von wenigstens einem der Primideale $\mathfrak{p}_i$ eine noch höhere als die in (138) angegebene Potenz in $\mathfrak{d}$ auf, was für D eine höhere als die ihr entsprechende Potenz der Reihe (139) als Faktor liefert, und demnach geht im gegenwärtigen Falle D durch eine höhere Potenz von p auf, als die

Potenz (140). Dies war aber genau der Inhalt des Satzes in Nr. 13.

Durch den gefundenen Hauptsatz ist die Zusammensetzung des Grundideals bezw. der Grundzahl völlig klargestellt bis auf diejenigen singulären Primfaktoren p, in deren Zerlegung in Primidealpotenzen sich durch p teilbare Exponenten befinden, bezüglich deren nur eine Mindestanzahl ermittelt ist, wie oft sie gewiß in der Grundzahl auftreten müssen. Da diese singulären Primzahlen nach Nr. 13 nur solche sein können, die in D wirklich aufgehen, ist ihre Anzahl nur eine ganz beschränkte, umsomehr, da sie zugleich $< n$ sein müssen, weil, wenn unter den Exponenten e_i einer durch p teilbar vorausgesetzt wird, nach der Formel

$$n = e_1 f_1 + e_2 f_2 + \cdots + e_r f_r$$

n größer als p wird. Hensel ist es gelungen, über die höchsten in D auftretenden Potenzen derselben noch näheren Aufschluß zu geben; im Anhange dieses Werkes kommen wir darauf zurück. Hier sollen zum Abschluß der voraufgehenden Betrachtungen nur noch zwei Bemerkungen über das Grundideal angefügt werden.

Bekanntlich ist die aus den Konjugierten von $\gamma_1, \gamma_2, \cdots, \gamma_n$ zusammengesetzte Determinante

$$\begin{vmatrix} \gamma_1, & \gamma_2, & \cdots, & \gamma_n \\ \gamma_1^{(1)}, & \gamma_2^{(1)}, & \cdots, & \gamma_n^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_1^{(n-1)}, & \gamma_2^{(n-1)}, & \cdots, & \gamma_n^{(n-1)} \end{vmatrix} = \sqrt{\mathrm{D}}.$$

Nennt man Γ_i den Koeffizienten von γ_i in der entwickelten Determinante, sodaß die Gleichung besteht:

$$\Gamma_1 \gamma_1 + \Gamma_2 \gamma_2 + \cdots + \Gamma_n \gamma_n = \sqrt{\mathrm{D}},$$

so erkennt man, wie schon die Vergleichung dieser Beziehung mit der für zwei komplementäre Basen im Kap. 1, Nr. 16 hergeleiteten Beziehung (96) zeigt, daß das zu γ_i komplementäre Element γ_i' gleich $\frac{\Gamma_i}{\sqrt{\mathrm{D}}}$ ist, während Γ_i als aus ganzen algebraischen Zahlen durch Additionen und Multiplikationen zusammengesetzt ebenfalls eine ganze algebraische Zahl sein

wird. Da hiernach die jedenfalls dem Körper angehörigen Zahlen $D\gamma_i'\gamma_k'$ auch ganze Zahlen also Zahlen in $\mathfrak{g}$ sein werden, so schließt man, daß der Modulus $D \cdot \mathfrak{g}'\mathfrak{g}'$ in $\mathfrak{g}$ enthalten ist. Zugleich aber ist

$$\mathfrak{g} \cdot D\mathfrak{g}'\mathfrak{g}' = D\mathfrak{g}\mathfrak{g}' \cdot \mathfrak{g}' = D\mathfrak{g}'\mathfrak{g}'$$

mithin der Modulus $D\mathfrak{g}'\mathfrak{g}'$ ein Ideal. Nennt man dasselbe $\mathfrak{d}_1$, so findet sich aus (135) durch Multiplikation mit $D\mathfrak{g}'$ die Gleichung

$$D\mathfrak{g}' = \mathfrak{d} \cdot \mathfrak{d}_1$$

also

$$D\mathfrak{g} = \mathfrak{d}^2 \cdot \mathfrak{d}_1$$

und daher der Satz: Die Grundzahl ist stets teilbar durch das Quadrat des Grundideales. Durch Übergang zu den Normen findet man aus vorstehender Gleichung mit Rücksicht auf $\mathfrak{N}(\mathfrak{d}) = D$ die fernere Gleichung

$$\mathfrak{N}(\mathfrak{d}_1) = D^{n-2}.$$

Wichtiger aber noch ist eine andere Bemerkung. Wir sind zwar durch die Dedekindschen Betrachtungen mittels der Gleichung (135) zum Grundideale geführt worden, doch tritt dessen Beziehung zur Grundzahl einigermaßen überraschend auf und seine eigentliche Bedeutung aus der definierenden Gleichung (135) noch nicht hervor. Um sie klar zu legen, denken wir uns zu den Basiszahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ von $\mathfrak{g}$ die Konjugierten und bilden aus ihnen die Differenzen

$$\begin{array}{llll} \gamma_1 - \gamma_1^{(1)}, & \gamma_2 - \gamma_2^{(1)}, & \cdots, & \gamma_n - \gamma_n^{(1)} \\ \gamma_1 - \gamma_1^{(2)}, & \gamma_2 - \gamma_2^{(2)}, & \cdots, & \gamma_n - \gamma_n^{(2)} \\ \cdot & \cdot & \cdot & \cdot \\ \gamma_1 - \gamma_1^{(n-1)}, & \gamma_2 - \gamma_2^{(n-1)}, & \cdots, & \gamma_n - \gamma_n^{(n-1)}. \end{array}$$

Sie sind sämtlich ganze algebraische Zahlen, die aber im allgemeinen nicht dem, der Betrachtung zum Grunde liegenden Körper $\mathfrak{K}$ angehören; man kann jedoch stets einen Körper $\mathfrak{K}'$ bilden, der sie sämtlich zugleich mit dem Körper $\mathfrak{K}$ in sich enthält, z. B. den Rationalitätsbereich, der aus ihnen und den Basiszahlen γ_i gebildet ist. In diesem endlichen Körper $\mathfrak{K}'$ bildet die Gesamtheit der Zahlen von der Form

$$\varphi_1(\gamma_1 - \gamma_1^{(1)}) + \varphi_2(\gamma_2 - \gamma_2^{(1)}) + \cdots + \varphi_n(\gamma_n - \gamma_n^{(1)}),$$

worin $\varphi_1, \varphi_2, \cdots, \varphi_n$ irgend welche ganze Zahlen in $\mathfrak{K}'$ sind, offenbar ein Ideal, welches durch das Zeichen

$$(141)\qquad \mathfrak{e}^{(1)} = \{\gamma_1 - \gamma_1^{(1)},\ \gamma_2 - \gamma_2^{(1)},\ \cdots,\ \gamma_n - \gamma_n^{(1)}\}'$$

ausgedrückt werde, und in gleicher Weise sind die entsprechend gebildeten Systeme

$$(141)\qquad \begin{cases} \mathfrak{e}^{(2)} = \{\gamma_1 - \gamma_1^{(2)},\ \gamma_2 - \gamma_2^{(2)},\ \cdots,\ \gamma_n - \gamma_n^{(2)}\}' \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{e}^{(n-1)} = \{\gamma_1 - \gamma_1^{(n-1)},\ \gamma_2 - \gamma_2^{(n-1)},\ \cdots,\ \gamma_n - \gamma_n^{(n-1)}\}' \end{cases}$$

Ideale des Körpers $\mathfrak{K}'$. Nach Hilbert[1]) mögen die so definierten Ideale (141) die Elemente des Körpers $\mathfrak{K}$ heißen. Sie haben eine nahe Beziehung zu seiner Fundamentalform

$$w_0 = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_n u_n,$$

insofern sie offenbar den Inhalt der $n - 1$ Formen

$$w_0 - w_0^{(1)},\ u_0 - w_0^{(2)},\ \cdots,\ w_0 - w_0^{(n-1)},$$

in denen $w_0^{(1)}, w_0^{(2)}, \cdots, w_0^{(n-1)}$ die Konjugierten der Fundamentalform sind, bedeuten. Nach dem allgemeinen Satze über den Inhalt eines Produktes von Formen (Nr. 3) ist demnach das Produkt der Ideale (141), welches selbst ein Ideal in $\mathfrak{K}'$ ist, dem Inhalte des Produktes

$$(142)\qquad (w_0 - w_0^{(1)})(w_0 - w_0^{(2)}) \cdots (w_0 - w_0^{(n-1)}),$$

d. i. demjenigen der Differente $\partial(w_0)$ gleich. Nennen wir $\alpha_1, \alpha_2, \cdots, \alpha_m$ die Koeffizienten derselben, so wäre das Produkt

$$(143)\qquad \mathfrak{e}^{(1)} \cdot \mathfrak{e}^{(2)} \cdots \mathfrak{e}^{(n-1)} = \{\alpha_1, \alpha_2, \cdots, \alpha_m\}'$$

nämlich die Gesamtheit der Zahlen von der Form

$$(144)\qquad \varphi_1\alpha_1 + \varphi_2\alpha_2 + \cdots + \varphi_m\alpha_m.$$

Nun gehören aber die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_m$ als symmetrische Funktionen der $n - 1$ zur erzeugenden Zahl konjugierten Zahlen dem Körper $\mathfrak{K}$ an; man kann daher das Ideal (143) auch als ein aus denselben Elementen α_i gebildetes Ideal

$$\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$$

1) Hilbert, Bericht über die Theorie der algebraischen Zahlkörper, im Jahresbericht der Deutschen Math. Vereinigung, 4. Bd. S. 200.

des Körpers $\mathfrak{K}$ auffassen, indem man die Koeffizienten φ_i in (144) auf ganze Zahlen des in $\mathfrak{K}'$ enthaltenen Körpers $\mathfrak{K}$ beschränkt. Nennt man $\mathfrak{d}_0$ das in solcher Weise aufgefaßte Ideal

$$\mathfrak{e}^{(1)} \cdot \mathfrak{e}^{(2)} \cdots \mathfrak{e}^{(n-1)},$$

so ist die mit bezug auf den Körper $\mathfrak{K}$ gebildete Norm desselben, d. i. $\mathfrak{N}(\mathfrak{d}_0)$ nach Nr. 5 mit der Norm der Differente ∂w_0, d. i. mit der Diskriminante der Fundamentalgleichung im Kroneckerschen Sinne äquivalent. Da diese letztere aber nach Nr. 7 auch mit der Grundzahl äquivalent ist, hat man zu schließen, daß die Grundzahl der Norm von $\mathfrak{d}_0$ gleich und daß das Ideal

$$\mathfrak{d}_0 = \mathfrak{e}^{(1)} \cdot \mathfrak{e}^{(2)} \cdots \mathfrak{e}^{(n-1)},$$

welches als Inhalt von ∂w_0 ein gemeinsamer Teiler aller Differenten $\partial \theta$, also ein Teiler des Grundideals ist, mit dem Grundideale $\mathfrak{d}$ identisch ist. Somit gilt der Satz: Das Grundideal ist der Inhalt der Differente der Fundamentalform oder im *Kronecker*schen Sinne dieser Differente äquivalent.

Achtes Kapitel.

Von den Einheiten.

1. Unter sämtlichen ganzen Zahlen eines Körpers $\mathfrak{K} = K(\mathsf{A}; R)$ sind seine Einheiten besonders hervorzuheben, und ihre vollständige Aufstellung ist von größter Wichtigkeit, u. a. für die Aufgabe, die Anzahl von Klassen äquivalenter Ideale des Körpers zu bestimmen. Deshalb wenden wir uns jetzt zunächst dazu, alle Einheiten zu ermitteln. Dirichlet gebührt der Ruhm, den ebenso durch seine Einfachheit wie durch seine Allgemeinheit ausgezeichneten Hauptsatz, welcher diese Aufgabe löst, zuerst gegeben und auf verhältnismäßig höchst einfache Weise bewiesen zu haben.

In jedem Körper sind die beiden „einfachen" Einheiten ± 1 vorhanden; im Körper ersten Grades, d. i. im Bereiche R aller rationalen Zahlen sind sie zugleich die einzigen Einheiten. Gleiches gilt im allgemeinen für den quadratischen Körper

der aus $\sqrt{d}$ gebildeten Zahlen, falls d negativ ist, denn wir haben gesehen, daß die Auffindung aller Einheiten eines quadratischen Körpers im wesentlichen übereinkommt mit der Ermittlung der ganzzahligen Auflösungen der Pellschen Gleichung

$$(1) \qquad x^2 - dy^2 = 1,$$

welche für $d < 0$ nur die beiden Lösungen $x = \pm 1$, $y = 0$ besitzt und so nur zu den genannten zwei Einheiten führt; ausnahmsweise gibt es in dem quadratischen Körper, wenn $d = -3$ ist, noch vier, wenn $d = -4$ ist, noch zwei weitere, stets also nur eine endliche Anzahl von Einheiten. Anders, wenn d positiv ist. Für diesen Fall hat zuerst Lagrange bewiesen und Dirichlet hat aus der einfachen, schon in Kap. 6, Nr. 8 ausgesprochenen Wahrheit, daß, wenn mehr als m Zahlen in m Intervalle sich verteilen, in wenigstens eins dieser Intervalle mehr als eine der Zahlen fallen muß, das gleiche Resultat hergeleitet, daß die Gleichung (1) eine von jener einfachen Lösung ± 1 verschiedene Auflösung zuläßt, woraus dann eine Einheit $x + y\sqrt{d}$ in dem quadratischen Körper entsteht, deren sämtliche Potenzen von einander verschieden sind, also unendlich viel Einheiten des Körpers darstellen. Eine weitere Untersuchung ließ sodann in einem solchen Körper das Vorhandensein einer fundamentalen Einheit erkennen, welche durch ihre positiven oder negativen ganzen Potenzen, mit ± 1 multipliziert, sämtliche im Körper vorhandenen Einheiten ergibt, und so war für ihn die oben gestellte Aufgabe vollständig gelöst.[1])

Eine geniale Erfassung der diesen Betrachtungen zum Grunde liegenden Prinzipien führte Dirichlet durch eine einfache Erweiterung des Gesichtskreises zur Auffindung seines großen, die Einheiten eines jeden Körpers beherrschenden Gesetzes.[2]) Drei Momente sind es, welche die hauptsächlichen

1) Vgl. Bachmann, Elemente der Zahlentheorie, S. 182 ff.

2) S. die in Kap. 5, Nr. 2 zitierten Arbeiten von Dirichlet. Die in ihnen nur skizzierte Theorie der Einheiten wurde zuerst von P. Bachmann, de unitatum complexarum theoria, Inaug.-Diss., Berlin 1864, ausführlich dargestellt.

Stützpunkte seiner Herleitung bilden, und deshalb von vornherein hervorgehoben werden sollen. Zunächst handelt es sich um den Nachweis einer Einheit von besonderer Beschaffenheit, durch welche es ermöglicht wird, mehrere von einander unabhängige Einheiten zu bestimmen; darauf wird gezeigt, daß eine endliche Anzahl unabhängiger Einheiten genügt, um durch ihre rationalen Potenzen alle Einheiten auszudrücken, und endlich, daß unter den verschiedenen Systemen solcher unabhängigen Einheiten ein fundamentales gewählt werden kann, deren ganze Potenzen bereits das Gleiche ergeben.

Indem wir dazu übergehen, diese Dirichletsche Theorie mit einigen, von Dedekind und Anderen daran angebrachten Modifikationen darzustellen, beschränken wir uns zunächst auf diejenigen Einheiten, welche in einer beliebig gegebenen „Ordnung in $\mathfrak{g}$“ enthalten sind. In Wahrheit ist solche Beschränkung nur eine scheinbare, denn im Gegenteil erhält man aus dem so für jede Ordnung sich findenden Resultate auch den für sämtliche Einheiten des Körpers giltigen Satz, da die Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen desselben nur eine spezielle Ordnung ist.

2. Sei also $\mathfrak{o}$ eine beliebige „Ordnung in $\mathfrak{g}$“ und ω_1, $\omega_2, \cdots, \omega_n$ irgend eine Basis derselben, sodaß

$$\mathfrak{o} = [\omega_1, \omega_2, \cdots, \omega_n]$$

gesetzt werden kann. Man bilde die Linearform

$$(2) \qquad w = u_1 \omega_1 + u_2 \omega_2 + \cdots + u_n \omega_n,$$

aus welcher man sämtliche Zahlen der Ordnung erhält, indem man die Unbestimmten u_i alle rationalen ganzen Zahlen annehmen läßt. Ist ω irgend eine Zahl in der Ordnung, so sind der Definition einer solchen gemäß auch die Produkte $\omega\omega_1$, $\omega\omega_2, \cdots, \omega\omega_n$ ebensolche Zahlen und daher bestehen n Gleichungen von der Form

$$(3) \qquad \omega\omega_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \cdots + a_{in}\omega_n \quad (i = 1, 2, \cdots, n)$$

mit ganzzahligen Koeffizienten und einer von Null verschiedenen Determinante derselben, da jene n Produkte ebenso wie

die n Basiszahlen ω_i selbst rational unabhängig sind. Diese Determinante ist übrigens, wie aus Kap. 1, Nr. 8 hervorgeht, nichts anderes als die Norm $N(\omega)$. Demgemäß werden die Produkte $N(\omega) \cdot \omega_i$ und allgemeiner das Produkt $N(\omega) \cdot \omega'$, wo ω' irgend eine Zahl der Ordnung bezeichnet, von der Gestalt

$$\omega(A_1 \omega_1 + A_2 \omega_2 + \cdots + A_n \omega_n)$$

mit ganzzahligen A_i, d. h. von der Gestalt $\omega \cdot \omega''$ sein, wo auch ω'' eine Zahl in $\mathfrak{o}$ bedeutet. So ergibt sich, welche Zahl der Ordnung unter ω' auch verstanden wird,

$$\frac{N(\omega)}{\omega} \cdot \omega'$$

als eine Zahl in $\mathfrak{o}$; da nun die Zahl ± 1 stets in $\mathfrak{o}$ enthalten ist, ersieht man hieraus für den Fall, daß ω eine Einheit der Ordnung d. i. eine Zahl ε in $\mathfrak{o}$, deren Norm gleich ± 1 ist, bedeutet, daß auch stets dann $\frac{1}{\varepsilon}$ eine Zahl dieser Ordnung ist, und, da ihre Norm ebenfalls gleich ± 1, eine Einheit derselben. Allgemeiner folgt sodann, daß jede positive oder negative Potenz einer Einheit in $\mathfrak{o}$ wieder eine Einheit der Ordnung ist.

Dies vorausgeschickt, betrachten wir die Konjugierten der Linearform (2). Indem wir hier je n einander konjugierte Größen durch Anfügung der oberen Indizes (1), (2), $\cdots$, (n) kennzeichnen wollen, schreiben wir sie

$$w^{(1)},\ w^{(2)},\ \cdots,\ w^{(n)}. \tag{2a}$$

Um sie zu erhalten, muß man auf die Gleichung

$$F(x) = 0$$

zurückgehen, durch deren Wurzeln der der Betrachtung zum Grunde liegende Körper und seine Konjugierten erzeugt werden; diese Wurzeln seien

$$\theta^{(1)},\ \theta^{(2)},\ \cdots,\ \theta^{(n)} \tag{4}$$

und unter ihnen gebe es r reelle und q Paare konjugiert imaginärer, sodaß

$$r + 2q = n; \tag{5}$$

wir setzen außerdem

$$r + q = s, \tag{6}$$

eine Zahl, die sich als besonders wichtig erweisen wird. Da wir von den bereits besprochenen Fällen $n = 1$ und $n = 2$, $r = 0$ in der Folge absehen können, dürfen wir stets $s \gtreqless 2$ voraussetzen. Die Wurzeln (4) mögen nun so geordnet werden, daß zuerst die r reellen genommen werden:

$$\theta^{(1)},\ \theta^{(2)},\ \cdots,\ \theta^{(r)},$$

dann aus jedem der q Paare konjugiert imaginärer Wurzeln nach Belieben eine derselben:

$$\theta^{(r+1)},\ \theta^{(r+2)},\ \cdots,\ \theta^{(r+q)},$$

endlich die ihnen konjugierten zweiten Glieder jedes Paares:

$$\theta^{(r+q+1)},\ \theta^{(r+q+2)},\ \cdots,\ \theta^{(r+2q)},$$

so daß stets $\theta^{(r+i)}$ und $\theta^{(r+q+i)}$ $(i = 1, 2, \cdots, q)$ konjugiert imaginäre Werte repräsentieren. Da der aus θ erzeugte Körper die Gesamtheit der aus θ rational gebildeten Zahlen ist, so werden die Konjugierten $\omega^{(1)}, \omega^{(2)}, \cdots, \omega^{(n)}$ einer Zahl ω desselben erhalten, indem man in ω die erzeugende Wurzel θ durch die sämtlichen Wurzeln (4) ersetzt. So finden sich die Konjugierten der Linearform w durch die Formel

$$w^{(i)} = u_1 \omega_1^{(i)} + u_2 \omega_2^{(i)} + \cdots + u_n \omega_n^{(i)}. \qquad (i = 1, 2, \cdots, n) \tag{7}$$

Ist die erzeugende Zahl θ des Körpers reell, so werden auch seine sämtlichen Zahlen reell sein, dagegen wird der Körper, wenn θ imaginär ist, mit θ zugleich auch imaginäre Zahlen enthalten. Demzufolge werden für $i = 1, 2, \cdots, r$ die Basiszahlen $\omega_1^{(i)}, \omega_2^{(i)}, \cdots, \omega_n^{(i)}$ reelle Werte bedeuten, für die größeren Werte des Index aber auch imaginär sein können in der Weise, daß stets $\omega_k^{(r+i)}$ und $\omega_k^{(r+q+i)}$ konjugiert imaginäre Werte bedeuten. Setzt man daher

$$\left\{\begin{aligned} &\mathfrak{f}_i = w^{(i)} \text{ für } i = 1, 2, \cdots, r \\ &\mathfrak{f}_{r+i} = \frac{w^{(r+i)} + w^{(r+q+i)}}{\sqrt{2}},\quad \mathfrak{f}_{r+q+i} = \frac{w^{(r+i)} - w^{(r+q+i)}}{\sqrt{-2}}, \\ &\text{für } i = 1, 2, \cdots, q \end{aligned}\right. \tag{8}$$

so werden die Ausdrücke

$$(8^a)\quad \begin{cases} \mathfrak{f}_1 = u_1\omega_1^{(1)} + u_2\omega_2^{(1)} + \cdots + u_n\omega_n^{(1)} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{f}_r = u_1\omega_1^{(r)} + u_2\omega_2^{(r)} + \cdots + u_n\omega_n^{(r)} \\ \mathfrak{f}_{r+1} = u_1\cdot\dfrac{\omega_1^{(r+1)}+\omega_1^{(r+\varrho+1)}}{\sqrt{2}} + \cdots + u_n\cdot\dfrac{\omega_n^{(r+1)}+\omega_n^{(r+\varrho+1)}}{\sqrt{2}} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{f}_{r+\varrho+1} = u_1\cdot\dfrac{\omega_1^{(r+1)}-\omega_1^{(r+\varrho+1)}}{i\sqrt{2}} + \cdots + u_n\cdot\dfrac{\omega_n^{(r+1)}-\omega_n^{(r+\varrho+1)}}{i\sqrt{2}} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{cases}$$

n Linearformen mit reellen Koeffizienten sein. Die Determinante $\varDelta$ dieser n Formen ist nach ihrem absoluten Werte gleich der Determinante

$$\begin{vmatrix} \omega_1^{(1)}, & \omega_2^{(1)}, & \cdots\cdots, & \omega_n^{(1)} \\ \cdot\ \cdot\ \cdot & & & \\ \omega_1^{(r+1)}, & \omega_2^{(r+1)}, & \cdots, & \omega_n^{(r+1)} \\ \cdot\ \cdot\ \cdot & & & \\ \omega_1^{(r+\varrho+1)}, & \omega_2^{(r+\varrho+1)}, & \cdots, & \omega_n^{(r+\varrho+1)} \\ \cdot\ \cdot\ \cdot & & & \end{vmatrix}$$

d. h. gleich der Quadratwurzel aus der Diskriminante $\varDelta(\mathfrak{o})$ der Ordnung; sie kann positiv gedacht werden, da man eventuell die Basiszahl $\omega_1^{(1)}$ nebst ihren Konjugierten mit entgegengesetztem Vorzeichen wählen darf.

Werden jetzt den Unbestimmten u_i irgend welche rational ganzzahlige Werte a_i beigelegt, so gehen die Linearformen $w^{(i)}$ in ein System konjugierter Zahlen über, deren eine der Ordnung $\mathfrak{o}$ angehört. Wir wollen die gedachten Zahlen a_i aber absolut nicht größer als k annehmen, wo k eine später genauer anzugebende positive ganze Zahl bezeichne. Dann wird offenbar allgemein für den entsprechenden Absolutwert von $\mathfrak{f}_i$ die Ungleichheit bestehen

$$|\mathfrak{f}_i| \overline{\gtrless} k(\Omega_1^{(i)} + \Omega_2^{(i)} + \cdots + \Omega_n^{(i)}),$$

wo $\Omega_h^{(i)}$ den absoluten Betrag des Koeffizienten von u_h im Ausdrucke von $\mathfrak{f}_i$ bedeutet, eine Größe, die lediglich von den Basiszahlen der Ordnung, nicht aber von der Wahl der Zahl k abhängig ist. Nennt man mithin Ω den größten Wert der den verschiedenen i entsprechenden Summen

$$\Omega_1^{(i)} + \Omega_2^{(i)} + \cdots + \Omega_n^{(i)},$$

so ist auch Ω eine nur von der Ordnung $\mathfrak{o}$ bestimmte Konstante, und für jeden Index $i = 1, 2, 3, \cdots, n$ ist

$$(9) \qquad |\mathfrak{f}_i| \overline{\overline{<}} k \cdot \Omega$$

d. h. der reelle Wert $\mathfrak{f}_i$ selbst zwischen den Grenzen $-k\Omega$ und $+k\Omega$ enthalten.

Nun denke man sich die n Funktionswerte $\mathfrak{f}_i$ beliebig in zwei Gruppen A, B verteilt, jedoch mit der Beschränkung, daß in jeder Gruppe sich wenigstens einer von ihnen und je zwei zusammengehörige Werte $\mathfrak{f}_{r+t}$, $\mathfrak{f}_{r+q+t}$ sich stets in derselben Gruppe finden sollen; die Anzahl der in der Gruppe A befindlichen Funktionswerte heiße σ, sodaß $n - \sigma$ der anderen Gruppe B anheimfallen. Richten wir unsere Aufmerksamkeit zunächst auf die σ Werte der ersten Gruppe. Da $n > \sigma > 0$ und $k > 0$ ist, sieht man leicht ein, daß

$$(k+1)^{\frac{n}{\sigma}} - k^{\frac{n}{\sigma}} > 1,$$

mithin zwischen dem Minuendus und dem Subtrahendus mindestens eine positive ganze Zahl m enthalten ist, für welche daher die Ungleichheiten

$$(10) \qquad (k+1)^n > m^\sigma > k^n$$

erfüllt sind. Setzt man dann

$$(11) \qquad d = \frac{2\Omega k}{m},$$

so ergibt sich

$$(12) \qquad d < 2\Omega \cdot k^{1-\frac{n}{\sigma}}.$$

Mittels dieser Zahl d läßt sich das Intervall von $-k\Omega$ bis $+k\Omega$ in m Teilintervalle von der gleichen Größe d und mit den bezüglichen Grenzen

$$(13) \qquad -k\Omega,\ -k\Omega + d;\ -k\Omega + d,\ -k\Omega + 2d;\ \cdots;$$
$$-k\Omega + (m-1)d,\ -k\Omega + md = k\Omega$$

zerlegen, denen man nach Belieben die oberen Grenzen zurechnen möge oder nicht. Wie man nun auch die ganzzahligen Werte der Unbestimmten u_i in der Reihe $0, 1, 2, \cdots, k$ wähle, was auf $(k+1)^n$ verschiedene Weisen geschehen kann, so

werden doch die σ dieser Wahl zugehörigen Funktionswerte $\mathfrak{f}_i$ der Gruppe A sich auf die m Intervalle (13) verteilen und, da jeder von ihnen in jedes der m Teilintervalle fallen kann, ist die Anzahl der möglichen Verteilungen gleich m^σ also kleiner als die Anzahl der möglichen Wahlen für die Unbestimmten, woraus zu schließen, daß für zwei verschiedene Wertsysteme dieser Unbestimmten aus der Reihe $0, 1, 2, \cdots, k$ die Verteilung der σ zugehörigen Funktionswerte in jene Teilintervalle die gleiche ist. Findet dies statt für die beiden Wertsysteme $u_i = a_i'$ und $u_i = a_i''$ der Unbestimmten, denen die Funktionswerte $\mathfrak{f}_i'$ bezw. $\mathfrak{f}_i''$ entsprechen mögen, so gehören dem Wertsysteme

$$u_i = a_i' - a_i''$$

der Unbestimmten, welche dann sämtlich numerisch nicht größer als k sind, die Funktionswerte

$$\mathfrak{f}_i = \mathfrak{f}_i' - \mathfrak{f}_i'' \qquad (i = 1, 2, \cdots, n) \tag{14}$$

zu, von welchen die zur Gruppe A gehörigen, da für sie $\mathfrak{f}_i', \mathfrak{f}_i''$ je in die gleichen Intervalle von der Größe d fallen, numerisch kleiner als d sein müssen. Nun ist $w^{(i)} = \mathfrak{f}_i$, wenn i der Reihe $1, 2, \cdots, r$ angehört, ferner ist wegen (8)

$$w^{(r+i)} = \frac{\mathfrak{f}_{r+i} + \sqrt{-1} \cdot \mathfrak{f}_{r+\varrho+i}}{\sqrt{2}}, \quad w^{(r+\varrho+i)} = \frac{\mathfrak{f}_{r+i} - \sqrt{-1} \cdot \mathfrak{f}_{r+\varrho+i}}{\sqrt{2}},$$

und daher sind die absoluten Beträge der Größen $w^{(r+i)}, w^{(r+\varrho+i)}$ gleich der Quadratwurzel aus

$$\frac{\mathfrak{f}_{r+i}^2 + \mathfrak{f}_{r+\varrho+i}^2}{2},$$

und somit besteht für diejenigen der Funktionswerte $w^{(i)}$, welche der Gruppe A entsprechen, durchweg die Ungleichheit

$$|w^{(i)}| < d, \tag{15}$$

während für die übrigen nach Formel (9) sich

$$|w^{(i)}| \lesseqgtr k\Omega \tag{15a}$$

ergibt. Da nun, wie bemerkt, die, ganzzahligen Werten der Unbestimmten u_i entsprechenden Werte $w^{(i)}$ die Konjugierten einer zur Ordnung $\mathfrak{o}$ gehörigen Zahl darstellen, ihr Produkt also der Norm der letzteren gleich ist, so erschließt man aus

dem Gesagten die Existenz einer Zahl ω in der Ordnung, für welche das Produkt P der Konjugierten $\omega^{(i)}$, welche der Gruppe A entsprechen, kleiner als d^σ, das Produkt Q der der Gruppe B entsprechenden nicht größer als $(k\Omega)^{n-\sigma}$, und für welche folglich die Norm

$$N(\omega) \text{ num.} < d^\sigma \cdot (k\Omega)^{n-\sigma}$$

d. i. mit Rücksicht auf (12)

$$(16) \qquad N(\omega) \text{ num.} < (2\Omega)^n$$

ist. Da aber diese Norm oder das Produkt PQ stets $\overline{\gtrless} 1$ ist, ergibt sich ferner dem absoluten Betrage nach $Q \overline{\gtrless} \frac{1}{P}$, d. i. $> d^{-\sigma}$; andererseits ist, wenn unter den Konjugierten $\omega^{(i)}$ eine der Gruppe B zugehörige Zahl ist, das Produkt der übrigen $n-\sigma-1$ Faktoren von Q absolut nicht größer als $(k\Omega)^{n-\sigma-1}$, folglich

$$|\,\omega^{(i)}\,| \overline{\gtrless} \frac{Q}{(k\Omega)^{n-\sigma-1}},$$

woraus durch Verbindung mit der letzten Ungleichheit und mit Rücksicht auf (12) die folgende hervorgeht:

$$(17) \qquad |\,\omega^{(i)}\,| > \frac{k}{(2\Omega)^{n-1}}.$$

Endlich kann, da $n > \sigma$ ist, die bisher unbestimmt gebliebene ganze Zahl k wegen (12) offenbar so groß gewählt werden, daß d kleiner als ein beliebig kleiner gegebener Wert a wird, zugleich aber $\frac{k}{(2\Omega)^{n-1}}$ größer als ein beliebig großer Wert b. Und so haben wir — alles in allem — zunächst folgendes festgestellt:

In der Ordnung $\mathfrak{o}$ gibt es eine Zahl ω, für welche die der Gruppe A entsprechenden Konjugierten $\omega^{(i)}$ dem absoluten Betrage nach kleiner als a, die der Gruppe B entsprechenden Konjugierten größer als b sind, während zugleich für ihre Norm die Ungleichheit (16) erfüllt ist.

3. Geht man nun aus von einer Zahl α in der Ordnung, deren Norm numerisch kleiner ist als $(2\Omega)^n$, wie eine solche nach dem eben Bewiesenen in $\mathfrak{o}$ sicherlich vorhanden ist, so

gibt es weiter eine Zahl β in der Ordnung, für deren Norm das Gleiche gilt, während zugleich die Konjugierten $\beta^{(i)}$, welche der Gruppe A entsprechen, absolut kleiner sind als der kleinste, die der Gruppe B entsprechenden absolut größer als der größte Absolutwert der Konjugierten von α. Desgleichen gibt es in $\mathfrak{o}$ eine Zahl γ, deren Norm wieder kleiner als $(2\Omega)^n$ ist, und deren zu A gehörige Konjugierten absolut kleiner, die zu B gehörigen absolut größer sind, als der kleinste resp. größte Absolutwert der Konjugierten von β; usw. So entsteht eine unbegrenzte Reihe ersichtlich verschiedener Zahlen $\alpha, \beta, \gamma, \cdots$ in $\mathfrak{o}$, deren Normen sämtlich numerisch kleiner sind als $(2\Omega)^n$. Jede Norm aber ist eine rationale ganze Zahl und zwischen $\pm(2\Omega)^n$ nur eine endliche Anzahl solcher Zahlen vorhanden, also müssen unendlich viele jener Zahlen ein- und dieselbe Norm N haben. Da diese letzteren Zahlen jedoch sämtlich von der Form (2) sind mit ganzzahligen Koeffizienten u_i, welche nur N (mod. N) verschiedene Reste lassen und somit nur N^n Restkombinationen (mod. N) für die Koeffizienten u_i verstatten, so muß es unter den gedachten Zahlen mindestens zwei geben, wir nennen die frühere derselben λ, die spätere μ, welche die gleiche Restkombination geben, in deren Differenz also die Koeffizienten durch N teilbar sind. Diese Differenz $\lambda - \mu$ selbst ist mithin eine durch N teilbare Zahl der Ordnung $\mathfrak{o}$:

$$(18) \qquad \lambda - \mu = N \cdot \omega,$$

wo auch ω eine Zahl in $\mathfrak{o}$. Aus dem im Eingange voriger Nummer Bemerkten folgt daher, daß die Zahl $\frac{N(\mu)}{\mu} \cdot \omega$ und, da die Eins stets eine Zahl der Ordnung ist, auch die folgende Zahl:

$$1 + \frac{N(\mu)}{\mu} \cdot \omega = 1 + \frac{N}{\mu} \cdot \omega$$

d. i. wegen (18) die Zahl $\frac{\lambda}{\mu}$ in der Ordnung enthalten und zwar, da $N\left(\frac{\lambda}{\mu}\right) = 1$ ist, eine Einheit in $\mathfrak{o}$ ist. Setzt man demgemäß $\frac{\lambda}{\mu} = \varepsilon$, mithin allgemein $\lambda^{(i)} = \mu^{(i)} \cdot \varepsilon^{(i)}$, so folgt aus der Bildung der Zahlen λ, μ, daß für diejenigen Indices i,

welche der Gruppe A entsprechen, $|\varepsilon^{(i)}| > 1$, dagegen für diejenigen, welche der Gruppe B entsprechen, $|\varepsilon^{(i)}| < 1$ ist. Man gewinnt demnach folgenden Satz:

In der Ordnung $\mathfrak{o}$ gibt es eine Einheit ε mit positiver Norm von der Art, daß die absoluten Beträge ihrer zur Gruppe A gehörigen Konjugierten größer, diejenigen ihrer zur Gruppe B gehörigen Konjugierten kleiner als Eins sind.

Hier führen wir eine Bezeichnung ein, von der wir mehrfachen Gebrauch machen werden. Wir setzen

$$\left\{\begin{aligned} c_i &= 1 && \text{für } i = 1, 2, \cdots, r \\ c_{r+i} &= c_{r+q+i} = 2 && \text{für } i = 1, 2, \cdots, q, \end{aligned}\right. \tag{19}$$

sodaß

$$c_1 + c_2 + \cdots + c_s = n \tag{20}$$

ist, und verstehen ferner, wenn α irgend eine Zahl des Körpers und $\alpha^{(i)}$ die zu α Konjugierten bedeutet, unter dem Zeichen $l_i(\alpha)$ den reellen Bestandteil von $c_i \log \alpha^{(i)}$; diese Ausdrücke $l_i(\alpha)$ sollen hinfort kurz die Logarithmen zu α genannt werden. Daraus geht offenbar die Beziehung

$$l_1(\alpha) + l_2(\alpha) + \cdots + l_s(\alpha) = \log |N(\alpha)| \tag{21}$$

hervor, welche für den Fall, daß α eine Einheit ε ist, die besondere Gestalt:

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_s(\varepsilon) = 0 \tag{22}$$

annimmt. Ist auch β eine Zahl des Körpers, so folgt zudem aus der Definition des Zeichens $l_i(\alpha)$ die Formel

$$l_i(\alpha\beta) = l_i(\alpha) + l_i(\beta). \tag{23}$$

Da nun der absolute Betrag von $\alpha^{(i)}$ gleich $e^{\frac{l_i(\alpha)}{c_i}}$ gefunden wird, so gestattet der obige Satz folgenden neuen Ausdruck: In der Ordnung $\mathfrak{o}$ gibt es eine Einheit ε mit positiver Norm von der Beschaffenheit, daß die zu ihr gehörigen Logarithmen $l_i(\varepsilon)$ positiv oder negativ sind, jenachdem der Index i der Gruppe A oder der Gruppe B entspricht.

4. Aus diesem Satze, welcher das erste Hauptmoment in der Dirichletschen Theorie bildet, fließt nun sogleich weiter der folgende Satz:

Es gibt in der Ordnung $\mathfrak{o}$ eine Anzahl von $s-1$ Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ mit positiver Norm von der Beschaffenheit, daß die Determinante

$$(24) \qquad L = \begin{vmatrix} l_{11}, & l_{12}, & \cdots, & l_{1,s-1} \\ l_{21}, & l_{22}, & \cdots, & l_{2,s-1} \\ \cdot & \cdot & \cdot & \cdot \\ l_{s-1,1}, & l_{s-1,2}, & \cdots, & l_{s-1,s-1} \end{vmatrix},$$

in welcher zur Abkürzung $l_{ik} = l_i(\varepsilon_k)$ gesetzt ist, einen positiven Wert hat. Das System S solcher $s-1$ Einheiten soll ein System unabhängiger Einheiten heißen. — Dieser Satz ist einleuchtend, wenn $s = 2$ ist, da alsdann

$$L = l_{11} = l_1(\varepsilon_1)$$

ist und, wenn wir der Gruppe A nur den ersten der Funktionswerte bezw. ihr erstes konjugiertes Paar, die übrigen der Gruppe B zurechnen, nach dem vorausgehenden Satze die Existenz einer Einheit ε_1 mit positiver Norm feststeht, für welche $l_1(\varepsilon_1) > 0$ ist. Nehmen wir also $s > 2$ an und setzen, indem wir unter m irgend eine Zahl zwischen 1 und s verstehen, voraus, daß man bereits $m-1$ Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{m-1}$ mit positiver Norm gefunden, für welche die Determinante

$$L' = \begin{vmatrix} l_{11}, & l_{12}, & \cdots, & l_{1,m-1} \\ l_{21}, & l_{22}, & \cdots, & l_{2,m-1} \\ \cdot & \cdot & \cdot & \cdot \\ l_{m-1,1}, & l_{m-1,2}, & \cdots, & l_{m-1,m-1} \end{vmatrix}$$

positiv ist. Dann ergibt sich aus demselben Satze die Existenz noch einer Einheit ε_m mit positiver Norm, für welche auch die folgende Determinante:

$$L'' = \begin{vmatrix} l_{11}, & l_{12}, & \cdots, & l_{1,m-1}, & l_{1,m} \\ l_{21}, & l_{22}, & \cdots, & l_{2,m-1}, & l_{2,m} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ l_{m-1,1}, & l_{m-1,2}, & \cdots, & l_{m-1,m-1}, & l_{m-1,m} \\ l_{m,1}, & l_{m,2}, & \cdots, & l_{m,m-1}, & l_{m,m} \end{vmatrix}$$

positiv ausfällt. In der Tat, entwickelt man diese Determinante nach den Elementen der letzten Kolonne, so wird

$$(25) \quad L'' = A_1 \cdot l_{1,m} + A_2 \cdot l_{2,m} + \cdots + A_{m-1} \cdot l_{m-1,m} + A_m \cdot l_{m,m},$$

und zugleich $\varDelta_m = L'$, nach der Voraussetzung also positiv sein. Teilt man aber der Gruppe A diejenigen Indizes i aus der Reihe $1, 2, \cdots, m$ zu, für welche $\varDelta_i > 0$ ist, nebst den ihnen etwa konjugierten Indizes $q + i$, welcher Gruppe dann mindestens ein Index, nämlich $i = m$ zugehören wird, der Gruppe B alle übrigen Indizes der gesamten Reihe $1, 2, \cdots, n$, welcher Gruppe dann, da $n \geqq s > m$ ist, ebenfalls ein Index i, nämlich $i = n$ zugehört, so leuchtet aus dem obigen Satze die Existenz einer Einheit ε_m mit positiver Norm ein, für welche in (25) die Multiplikatoren derjenigen $\varDelta_i$, welche positiv sind, gleichfalls positiv, die der übrigen negativ sind, und demnach der ganze Ausdruck L'' positiv sein wird, w. z. b. w. Nun gibt es zunächst nach dem für den Fall $s = 2$ Bemerkten eine Einheit ε_1 mit positiver Norm, für welche

$$l_{11}$$

positiv ist; dem Bewiesenen zufolge ist also auch eine Einheit ε_2 mit positiver Norm vorhanden, für welche die Determinante

$$\begin{vmatrix} l_{11}, & l_{12} \\ l_{21}, & l_{22} \end{vmatrix}$$

positiv ausfällt, daher wieder eine Einheit ε_3 mit positiver Norm, welche die Determinante

$$\begin{vmatrix} l_{11}, & l_{12}, & l_{13} \\ l_{21}, & l_{22}, & l_{23} \\ l_{31}, & l_{32}, & l_{33} \end{vmatrix}$$

positiv macht usw. Da man aber in dieser Richtung fortgehen kann bis zur größten Zahl $m < s$, d. i. bis $m = s - 1$, so ist der ausgesprochene zweite Hauptsatz erwiesen.

5. Eine andere Herleitung dieses Satzes gab Minkowski in einer kleinen Note (Göttinger Nachrichten, 1900, p. 90). Sie stützt sich auf einen bemerkenswerten Determinantensatz, der folgendermaßen lautet:

Sind in einer Determinante

$$|a_{ik}| \quad (i, k = 1, 2, \cdots, m)$$

mit reellen Elementen alle Glieder außerhalb der Hauptdiagonale negativ, dagegen die Summe

$$s_h = a_{h1} + a_{h2} + \cdots + a_{hm} \qquad (h = 1, 2, \cdots, m) \tag{26}$$

der Glieder in jeder Horizontalreihe positiv, so ist der Wert der Determinante gleichfalls positiv. Der Satz setzt eigentlich $m > 1$ voraus, da sonst kein Glied außerhalb der Diagonale vorhanden ist, doch ist für $m = 1$ die Determinante mit ihrem einzigen Elemente a_{11} identisch, also zugleich auch positiv. Ist dagegen $m = 2$, also

$$s_1 = a_{11} + a_{12}, \quad s_2 = a_{21} + a_{22}$$

positiv, so folgt

$$|a_{ik}| = a_{22}s_1 - a_{12}s_2,$$

mithin den Voraussetzungen zufolge positiv. Hieraus ergibt sich der allgemeine Satz durch vollständige Induktion. Nimmt man ihn nämlich als bewiesen an für alle Determinanten geringeren Grades als m, und setzt in der Determinante $|a_{ik}|$ für a_{hh} die Summe $s_h + \alpha_{hh}$, so ist offenbar α_{hh} positiv und die Summe

$$a_{h1} + \cdots + \alpha_{hh} + \cdots + a_{hm} = 0, \qquad (h = 1, 2, \cdots, m) \tag{27}$$

woraus folgt, daß auch die Determinante

$$\begin{vmatrix} \alpha_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & \alpha_{22}, & \cdots, & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1}, & a_{m2}, & \cdots, & \alpha_{mm} \end{vmatrix} = 0$$

ist. Entwickelt man daher die Determinante

$$|a_{ik}| = \begin{vmatrix} s_1 + \alpha_{11}, & a_{12}, & \cdots, & a_{1m} \\ a_{21}, & s_2 + \alpha_{22}, & \cdots, & a_{2m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1}, & a_{m2}, & \cdots, & s_m + \alpha_{mm} \end{vmatrix}$$

nach den Größen s_i, so verschwindet das von diesen Größen freie Glied, das Glied mit $s_1 s_2 \cdots s_m$ hat den Koeffizienten 1, jedes andere aber einen positiven Koeffizienten, da z. B. der Koeffizient von $s_1 s_2$ die Determinante

$$\begin{vmatrix} \alpha_{33}, & a_{34}, & \cdots, & a_{3m} \\ a_{43}, & \alpha_{44}, & \cdots, & a_{4m} \\ \cdot & \cdot & \cdot & \cdot \\ a_{m3}, & a_{m4}, & \cdots, & \alpha_{mm} \end{vmatrix}$$

ist, in welcher alle Elemente außerhalb der Diagonale negativ sind, und wegen (27) die Summe aller Glieder einer Reihe sicher positiv ist; nach der Voraussetzung ist also auch der Wert dieser Determinante positiv. Somit sind sämtliche Glieder der Entwicklung und mit ihnen die Determinante $|a_{ik}|$ selbst positiv, w. z. b. w.

Nun gibt es nach Nr. 3 in der Ordnung $\mathfrak{o}$ eine Einheit ε mit positiver Norm von der Beschaffenheit, daß unter den Logarithmen

$$l_1(\varepsilon),\ l_2(\varepsilon),\ \cdots,\ l_{s-1}(\varepsilon),\ l_s(\varepsilon)$$

nach Belieben ein bestimmter positiv, alle übrigen negativ sind. Demnach lassen sich $m = s - 1$ Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m$ mit positiver Norm so bestimmen, daß allgemein für die Einheit ε_i von den zugehörigen Logarithmen der Logarithmus $l_i(\varepsilon_i) > 0$, alle übrigen negativ sind, sodaß wegen der für jede Einheit ε_i stattfindenden Beziehung

$$l_1(\varepsilon_i) + l_2(\varepsilon_i) + \cdots + l_s(\varepsilon_i) = 0$$

jedenfalls

$$l_1(\varepsilon_i) + l_2(\varepsilon_i) + \cdots + l_m(\varepsilon_i) > 0$$

ist. Mittels des Hilfssatzes erschließt man aus diesen Bestimmungen sogleich das Bestehen der Ungleichheit

$$\begin{vmatrix} l_1(\varepsilon_1), & l_2(\varepsilon_1), & \cdots, & l_m(\varepsilon_1) \\ l_1(\varepsilon_2), & l_2(\varepsilon_2), & \cdots, & l_m(\varepsilon_2) \\ \cdot & \cdot & \cdot & \cdot \\ l_1(\varepsilon_m), & l_2(\varepsilon_m), & \cdots, & l_m(\varepsilon_m) \end{vmatrix} > 0,$$

welche lehrt, daß die zuvor charakterisierten Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m$ ein System von $m = s - 1$ unabhängigen Einheiten der Ordnung $\mathfrak{o}$ darstellen.

Man bemerke, daß, während die in der vorigen Nummer gegebene Dirichletsche Methode zur Bestimmung eines solchen Systems die Bildung gewisser Determinanten verlangt, die sich aus den successive schon ermittelten Einheiten zusammensetzen, hier die Ermittlung der einzelnen Einheiten nach Nr. 3 ganz direkt und unabhängig voneinander geschieht.

6. Wir haben bisher die Dirichletsche Theorie im wesentlichen in der Darstellung vorgetragen, die Dedekind ihr gegeben hat. Bevor wir aber ihre Entwicklung zu Ende führen

halten wir bei der großen Bedeutung, die ihr zukommt, es für geboten, sie nach Minkowski's Vorgange auf eine noch breitere Grundlage zu stellen. Diese Grundlage bildet der folgende elegante und durch seine Allgemeinheit ausgezeichnete Satz:

Sind

$$F_i = r_{i1}u_1 + r_{i2}u_2 + \cdots + r_{in}u_n \quad (i = 1, 2, \cdots, n) \tag{28}$$

n homogene lineare Funktionen der n Unbestimmten u_i mit beliebigen reellen Koeffizienten, deren Determinante $|r_{ik}|$ gleich 1 ist, so können den Unbestimmten solche ganzzahlige, nicht durchweg verschwindende Werte beigelegt werden, daß die sämtlichen Funktionen absolut $\overline{\gtrless} 1$ werden.

Im Wesen mit diesem Satze identisch, doch allgemeiner in der Ausdrucksweise ist offenbar der andere Satz: Ist Δ die (positiv vorausgesetzte) Determinante der Funktionen (28) und bedeuten $k_1, k_2, \cdots, k_n$ beliebige positive Konstanten, deren Produkt gleich Δ ist, so können den Unbestimmten solche nicht sämtlich verschwindende ganzzahlige Werte erteilt werden, daß für die Funktionen (28) die n Ungleichheiten

$$|F_i| \overline{\gtrless} k_i \quad (i = 1, 2, \cdots, n)$$

erfüllt sind. Dividiert man nämlich in der jetzigen Voraussetzung die Formen (28) bezw. durch k_i, so erhält man in den Formen $\frac{F_i}{k_i}$ n Funktionen von der Art des ersten Satzes, für welche also dann der Absolutwert von $\frac{F_i}{k_i}$ gleich oder kleiner als 1 gemacht werden kann.

Minkowski hat (s. Geometrie der Zahlen, Kap. 4) diesen fundamentalen Satz aus allgemeinen „zahlengeometrischen“ Grundsätzen gewonnen, auf die hier einzugehen nicht der Ort ist. Aber Hurwitz[1]) ist es gelungen, ihn direkt zu beweisen,

1) Hurwitz, über lineare Formen mit ganzzahligen Variablen, Götting. Nachr. 1897.

indem er — beachtenswerter Weise — ihn genau demselben einfachen Prinzip entnimmt, dem auch die Dirichletsche Theorie entsprungen ist. Wir geben dieser Herleitung durch Hurwitz hier Raum.

Fassen wir die n Unbestimmten u_i als die Basis eines n-gliedrigen Modulus

$$\mathfrak{m} = [u_1, u_2, \cdots, u_n]$$

auf und setzen, indem wir zunächst die r_{ik} ganzzahlig voraussetzen

$$v_i = r_{1i}u_1 + r_{2i}u_2 + \cdots + r_{ni}u_n, \tag{29}$$

so ist der Modulus

$$\mathfrak{n} = [v_1, v_2, \cdots, v_n]$$

in $\mathfrak{m}$ enthalten und nach Kap. 2, Nr. 6 ist die Anzahl der Klassen, in welche die Zahlen von $\mathfrak{m}$ sich in bezug auf den Modulus $\mathfrak{n}$ verteilen, nämlich $(\mathfrak{m}, \mathfrak{n})$, gleich dem Absolutwerte der Determinante der Gleichungen (29) für $i = 1, 2, \cdots, n$, d. h. gleich Δ. Ist nun k die größte ganze Zahl unterhalb $\sqrt[n]{\Delta}$, sodaß

$$k^n \gtreqless \Delta < (k+1)^n$$

ist, und legt man in der Form

$$C_1u_1 + C_2u_2 + \cdots + C_nu_n$$

den Koeffizienten C_i alle ganzzahligen Werte $0, 1, 2, \cdots, k$ bei, so erhält man $(k+1)^n$ Zahlen des Modulus $\mathfrak{m}$, die, weil $(k+1)^n > \Delta$ ist, nicht sämtlich inkongruent sein können (mod. $\mathfrak{n}$); demnach müssen zwei von ihnen,

$$C_1'u_1 + C_2'u_2 + \cdots + C_n'u_n, \quad C_1''u_1 + C_2''u_2 + \cdots + C_n''u_n$$

einander kongruent und daher ihre Differenz

$$C_1u_1 + C_2u_2 + \cdots + C_nu_n,$$

in welcher allgemein die nicht sämtlich verschwindenden Zahlen $C_i = C_i' - C_i''$ numerisch nicht größer als k, umsomehr also nicht größer als $\sqrt[n]{\Delta}$ sind, eine Zahl des Modulus $\mathfrak{n}$ sein, mithin eine Gleichung bestehen

$$C_1u_1 + C_2u_2 + \cdots + C_nu_n = x_1v_1 + x_2v_2 + \cdots + x_nv_n,$$

in welcher die x_i rationale ganze Zahlen bedeuten. Diese zerfällt aber mit Rücksicht auf die Werte (29) der v_i in die folgenden Gleichungen:

$$C_i = r_{i1}x_1 + r_{i2}x_2 + \cdots + r_{in}x_n, \quad (i = 1, 2, \cdots, n)$$

welche lehren, daß den Unbestimmten u_i in den Formen (28) solche ganzzahlige Werte x_i beigelegt werden können, daß die entstehenden Werte C_i der Formen numerisch nicht größer ausfallen als $\sqrt[n]{\Delta}$, vorausgesetzt, daß die Koeffizienten r_{ik} der Formen ganzzahlig sind. Diese Werte x_i können nicht sämtlich Null sein, da die mit C_i bezeichneten Differenzen es ebenfalls nicht waren.

Dasselbe gilt aber auch noch, wenn die Koeffizienten r_{ik} nur rational sind. Denn, ist dann g ihr Generalnenner, so werden dem eben Bewiesenen zufolge die n ganzzahligen Formen

$$g(r_{i1}u_1 + r_{i2}u_2 + \cdots + r_{in}u_n), \quad (i = 1, 2, \cdots, n)$$

deren Determinante $g^n\Delta$ ist, für passende ganzzahlige, nicht sämtlich der Null gleiche Werte $u_i = x_i$ numerisch nicht größer als $\sqrt[n]{g^n\Delta}$ und somit die Formen (28) selbst nicht größer als $\sqrt[n]{\Delta}$, w. z. b. w.

Endlich gilt es aber auch noch, wenn die Koeffizienten r_{ik} beliebig reell sind. Jeden solchen Wert r_{ik} darf man nämlich als den Grenzwert betrachten, gegen welchen eine gewisse unbegrenzte Reihe

$$r'_{ik}, \quad r''_{ik}, \quad r'''_{ik}, \quad \cdots$$

numerisch wachsender rationaler Werte konvergiert. So ergeben sich unendlich viel Systeme von je n linearen Formen

$$r^{(\lambda)}_{i1}u_1 + r^{(\lambda)}_{i2}u_2 + \cdots + r^{(\lambda)}_{in}u_n, \quad (i = 1, 2, \cdots, n)$$

deren Determinanten $\Delta^{(\lambda)}$ offenbar mit unbegrenzt wachsendem λ gegen die Grenze Δ konvergieren, derart, daß, wenn Δ_1, Δ_2 zwei Größen bezeichnen, deren erste nur beliebig wenig kleiner, die zweite nur beliebig wenig größer ist als Δ, von einem endlichen Werte λ_0 des Index λ an $\Delta^{(\lambda)}$ stets zwischen Δ_1, Δ_2 enthalten bleibt. Für jedes der diesen letzteren Werten λ entsprechenden Systeme von n Formen gibt es dem bereits Be-

wiesenen zufolge ganzzahlige, nicht sämtlich verschwindende Werte $u_i = x_i^{(\lambda)}$ der Unbestimmten von der Beschaffenheit, daß sämtliche Ausdrücke

$$F_i^{(\lambda)} = r_{i1}^{(\lambda)} x_1^{(\lambda)} + r_{i2}^{(\lambda)} x_2^{(\lambda)} + \cdots + r_{in}^{(\lambda)} x_n^{(\lambda)} \quad (i = 1, 2, \cdots, n) \tag{30}$$

numerisch nicht größer sind als $\sqrt[n]{\Delta^{(\lambda)}}$, folglich auch nicht größer als $\sqrt[n]{\Delta_2}$. Man bezeichne die Auflösung der vorstehenden n Gleichungen durch die Formeln

$$x_k^{(\lambda)} = \varrho_{1k}^{(\lambda)} F_1^{(\lambda)} + \varrho_{2k}^{(\lambda)} F_2^{(\lambda)} + \cdots + \varrho_{nk}^{(\lambda)} F_n^{(\lambda)} \quad (k = 1, 2, \cdots, n) \tag{31}$$

und nenne r den Absolutwert des größten unter den Koeffizienten r_{ik}, sodaß von jenem endlichen Werte λ_0 des Index λ an auch jedes $r_{ik}^{(\lambda)}$ numerisch kleiner ist als r. Da $\varrho_{ik}^{(\lambda)}$ eine Unterdeterminante $n - 1^{\text{ter}}$ Ordnung der Determinante der Gleichungen (30) ist, geteilt durch diese Determinante selbst, so ist es gewiß kleiner als $\frac{r^{n-1}}{\Delta_1}$ mal der Anzahl der Glieder, deren Aggregat eine solche Unterdeterminante ist, also kleiner als $(n-1)!\,\frac{r^{n-1}}{\Delta_1}$. Wegen (31) folgt hieraus

$$x_k^{(\lambda)} \quad \text{numerisch} \quad < n!\,\frac{r^{n-1}}{\Delta_1} \cdot \sqrt[n]{\Delta_2}\,.$$

Diese Ungleichheit, deren obere Grenze ein fester, nur durch die Koeffizienten der n Formen (28) bestimmter, endlicher Wert ist, lehrt, daß jedes der Systeme ganzer Zahlen

$$x_1^{(\lambda)},\ x_2^{(\lambda)}, \cdots, x_n^{(\lambda)},$$

für welche die n Ungleichheiten

$$r_{i1}^{(\lambda)} x_1^{(\lambda)} + r_{i2}^{(\lambda)} x_2^{(\lambda)} + \cdots + r_{in}^{(\lambda)} x_n^{(\lambda)} \ \text{num.} \ \overline{\gtrless}\ \sqrt[n]{\Delta^{(\lambda)}}, \quad (\lambda > \lambda_0) \quad (i = 1, 2, \cdots, n)$$

erfüllt sind, sich nur unter einer endlichen Anzahl gewisser Systeme von n ganzen, nicht durchweg der Null gleichen Zahlen $x_1, x_2, \cdots, x_n$ befinden kann, und daß somit wenigstens durch eins dieser letzteren Systeme notwendig die Ungleichheiten

$$r_{i1}^{(\lambda)}x_1 + r_{i2}^{(\lambda)}x_2 + \cdots + r_{in}^{(\lambda)}x_n \text{ num. } \overline{\gtrless} \sqrt[n]{\Delta^{(\lambda)}}$$
$$(i = 1, 2, \cdots, n)$$

für unendlich viel Werte des Index $\lambda > \lambda_0$ erfüllt sein müssen. Läßt man λ aber diese unbegrenzte Reihe von Werten durchlaufen, so ergibt sich schließlich durch den Übergang zur Grenze $\lambda = \infty$ das System der Ungleichheiten:

$$(32) \qquad r_{i1}x_1 + r_{i2}x_2 + \cdots + r_{in}x_n \text{ num. } \overline{<} \sqrt[n]{\Delta}$$
$$(i = 1, 2, \cdots, n)$$

d. h. das Vorhandensein eines Systems ganzer Zahlen $x_1, x_2, \cdots, x_n$ von der Eigenschaft, wie sie nachgewiesen werden sollte.

Auf solche Weise ist ein Satz begründet worden, der offenbar ein Spezialfall des zweiten der vorangestellten Sätze ist, seinerseits aber den ersten derselben, der durch die besondere Annahme $\Delta = 1$ aus ihm hervorgeht, als besonderen Fall in sich enthält. Da diesem aber, wie bemerkt, der an zweiter Stelle gegebene gleichwertig ist, so leuchtet ein, daß mit dem eben nach Hurwitz abgeleiteten Satze zugleich auch der letztere bewiesen worden ist.

Genauer kann das System der Zahlen x_i so bestimmt werden, daß in $n-1$ der Formeln (32), etwa in den $n-1$ letzten derselben nur das Ungleichheitszeichen gilt. Dies beweist Hurwitz a. a. O. folgendermaßen. Für jeden Wert des Index λ bestimme man eine positive Größe $\delta_\lambda < \sqrt[n]{\Delta}$ in solcher Weise, daß die unbegrenzte Reihe dieser Größen gegen Null konvergiert, und eine entsprechende, ebenfalls positive Größe δ_λ', welche durch die Bedingung

$$\left(\sqrt[n]{\Delta} + \delta_\lambda'\right) \cdot \left(\sqrt[n]{\Delta} - \delta_\lambda\right)^{n-1} = \Delta$$

mit der ersteren verknüpft ist und daher mit wachsendem λ auch die Null zur Grenze haben wird. Wählt man nun in der zweiten Fassung des Minkowskischen Satzes die Konstanten

$$k_1 = \sqrt[n]{\Delta} + \delta_\lambda', \quad (\text{für } i > 1) \quad k_i = \sqrt[n]{\Delta} - \delta_\lambda,$$

so gibt es diesem Satze gemäß ein nicht verschwindendes System ganzer Zahlen x_i von der Beschaffenheit, daß

$$r_{11}x_1 + r_{12}x_2 + \cdots + r_{1n}x_n \overline{<} \sqrt[n]{\Delta} + \delta_\lambda'$$

für $i > 1$ aber

$$r_{i1}x_1 + r_{i2}x_2 + \cdots + r_{in}x_n \overline{\gtrless} \sqrt[n]{\varDelta} - \delta_\lambda < \sqrt[n]{\varDelta}$$

wird. Analog den voraufgehenden Betrachtungen gibt es sogar ein System ganzer Zahlen x_i, welches diesen Ungleichheiten für unendlich viel Werte des Index λ genügt. Indem man λ also diese Werte durchlaufen läßt, erkennt man als Resultat des Grenzüberganges das Bestehen der Ungleichheiten

$$r_{11}x_1 + r_{12}x_2 + \cdots + r_{1n}x_n \overline{\gtrless} \sqrt[n]{\varDelta},$$

für $i > 1$:

$$r_{i1}x_1 + r_{i2}x_2 + \cdots + r_{in}x_n < \sqrt[n]{\varDelta},$$

wie zu beweisen war. — Eine andere Begründung dieses präziseren Satzes findet der Leser in Hilberts Bericht über die Theorie der alg. Zahlkörper, Deutsche Math. Verein., 4. Bd. 1897, p. 212.

7. Wir ziehen aus diesen Ergebnissen zuvörderst zwei wichtige Folgerungen, welche die Grundzahl eines Körpers betreffen. Die Grundzahl ist nämlich immer, abgesehen vom Körper der rationalen Zahlen, als dessen Grundzahl die Einheit anzusehen ist, von ± 1 verschieden, und es ist ferner unter den Körpern gleichen Grades nur eine endliche Anzahl solcher vorhanden, die ein- und dieselbe Grundzahl besitzen.

Um den ersteren Satz zu beweisen, aus welchem hervorgeht, daß es, um mit Minkowski zu sprechen (Geometrie der Zahlen, p. 129), stets mindestens eine kritische Primzahl, d. i. eine Primzahl gibt, die in der Grundzahl des Körpers aufgeht, kann man verfahren, wie folgt. Unter den Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ in Nr. 2 verstehe man jetzt nicht die Basis einer beliebigen, sondern der besonderen Ordnung $\mathfrak{g}$ aller ganzen Zahlen des Körpers, sodaß die Formel

$$w = u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n$$

jede ganze Zahl desselben liefert, wenn man die u_i alle rationalen ganzen Zahlen durchlaufen läßt; $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$ seien wieder die n Konjugierten dieser Form; für ganzzahlige Werte der u_i repräsentieren sie n konjugierte ganze algebraische Zahlen, deren eine dem Körper angehört. Die n linearen

Formen (8^a) sind jetzt Funktionen der u_i mit reellen Koeffizienten, deren Determinante Δ der Absolutwert der Quadratwurzel aus der **Grundzahl** des Körpers ist. Man wähle die n positiven Konstanten

$$C_i \text{ für } i = 1, 2, \cdots, r \quad \text{und} \quad C_{r+i} = C_{r+q+i} \quad \text{für } i = 1, 2, \cdots, q, \tag{33}$$

was offenbar auf unendlich viel Weisen geschehen kann, so, daß

$$C_1 C_2 \cdots C_r C_{r+1} \cdots C_n = 1 \tag{34}$$

wird, und setze

$$k_i = C_i \sqrt[n]{\Delta} \tag{35}$$

Will man nun den letzten, präziseren Satz der vorigen Nummer benutzen, so darf man schließen, daß für die Unbestimmten in den Formen (8^a) solche, nicht sämtlich verschwindende ganzzahlige Werte gesetzt werden können, daß dem absoluten Betrage nach die Ungleichheit

$$\mathfrak{f}_h \mathrel{\overline{\overline{<}}} k_h \text{ d. i. } \mathrel{\overline{\overline{<}}} C_h \sqrt[n]{\Delta}, \tag{36}$$

für die übrigen $\mathfrak{f}_i$ aber die Ungleichheiten

$$\mathfrak{f}_i < k_i \text{ d. i. } < C_i \sqrt[n]{\Delta} \tag{37}$$

bestehen. Ist der, der Betrachtung zugrunde liegende Körper ein reeller Körper, für den etwa die Zahlen $\omega_1^{(1)}, \omega_2^{(1)}, \cdots, \omega_n^{(1)}$ die Basis ausmachen, so wähle man für $\mathfrak{f}_h$ die Form $\mathfrak{f}_1$, im entgegengesetzten Falle, in welchem der Körper etwa die Basis $\omega_1^{(r+1)}, \omega_2^{(r+1)}, \cdots, \omega_n^{(r+1)}$ habe, wähle man nach Belieben für $\mathfrak{f}_h$ eine der beiden Formen $\mathfrak{f}_{r+1}, \mathfrak{f}_{r+q+1}$. Da der absolute Betrag der ganzen Zahl $w^{(i)}$, welche den vorher bezeichneten ganzzahligen Werten der Unbestimmten zugehört, für $i = 1, 2, \cdots, r$ demjenigen von $\mathfrak{f}_i$ gleich, andernfalls gleich

$$\sqrt{\frac{\mathfrak{f}_{r+i}^2 + \mathfrak{f}_{r+q+i}^2}{2}}$$

ist, so findet sich der absolute Betrag des Produktes

$$\mathfrak{f}_1 \mathfrak{f}_2 \cdots \mathfrak{f}_r \cdot \frac{\mathfrak{f}_{r+1}^2 + \mathfrak{f}_{r+q+1}^2}{2} \cdots \frac{\mathfrak{f}_{r+q}^2 + \mathfrak{f}_{r+2q}^2}{2} \tag{38}$$

demjenigen der Norm $N(w)$ gleich, mithin $\overline{>} 1$. Andererseits sieht man mit Beachtung der Gleichungen (33) bis (35) sowie der Ungleichheiten (36) und (37), daß er kleiner ist als

$$k_1 k_2 \cdots k_n = C_1 C_2 \cdots C_n \cdot \Delta = \Delta,$$

und daraus folgt, wie behauptet, $\Delta > 1$.

Auf Grund des ungenaueren vorletzten Satzes der vorigen Nummer würden sich statt der Ungleichheiten (36) und (37) nur die folgenden:

$$\mathfrak{k}_i \overline{<} k_i \text{ d. i. } C_i \sqrt[n]{\Delta} \qquad (39)$$
$$(i = 1, 2, \cdots, n)$$

und hieraus weiter schließen lassen, daß der absolute Betrag des Produktes (38) nicht größer sei als Δ. Mithin wäre er, falls die Grundzahl des Körpers ± 1 wäre, nicht größer als 1; da er aber schon nicht kleiner als 1 gefunden wurde, so müßte er gleich 1 sein. Nun ist jenes Produkt, wie die Beachtung der Formeln (33), (34) lehrt, dem folgenden gleich:

$$\frac{w^{(1)}}{C_1} \cdot \frac{w^{(2)}}{C_2} \cdots \frac{w^{(r)}}{C_r} \cdot \frac{w^{(r+1)} w^{(r+\varrho+1)}}{C_{r+1} C_{r+\varrho+1}} \cdots \frac{w^{(r+\varrho)} w^{(r+2\varrho)}}{C_{r+\varrho} C_{r+2\varrho}}.$$

Also müßte von den absoluten Beträgen seiner Faktoren entweder mindestens einer, der von $\frac{w^{(i)}}{C_i}$, größer als 1, oder sie sämtlich gleich 1 sein. Ist im ersten Falle $i \overline{<} r$, so wäre wegen $w^{(i)} = \mathfrak{k}_i$ auch $\frac{\mathfrak{k}_i}{C_i}$, also nach (39) umsomehr auch Δ gegen die Annahme größer als 1; wäre dagegen etwa $i = r + 1$, also der Absolutbetrag von $\frac{w^{(r+1)}}{C_{r+1}}$, welcher demjenigen von $\frac{w^{(r+\varrho+1)}}{C_{r+\varrho+1}}$ gleich, nämlich gleich

$$\sqrt{\frac{1}{2}\left(\frac{\mathfrak{k}^2_{r+1}}{C^2_{r+1}} + \frac{\mathfrak{k}^2_{r+\varrho+1}}{C^2_{r+\varrho+1}}\right)}$$

ist, größer als 1, so folgte auch der Absolutbetrag eines der beiden Quotienten $\frac{\mathfrak{k}_{r+1}}{C_{r+1}}, \frac{\mathfrak{k}_{r+\varrho+1}}{C_{r+\varrho+1}}$ größer als 1 und deshalb wieder gegen die Annahme $\Delta > 1$. Es bleibt also nur der zweite Fall. In diesem wären die absoluten Beträge der

Zahlen $w^{(i)}$ sämtlich bezw. gleich C_i; da nun $w^{(i)}$ also auch der konjugiert imaginäre Wert eine ganze algebraische Zahl ist, so ist's auch ihr Produkt, d. h. C_i^2 und folglich wäre es auch C_i. Indessen darf man von den Konstanten $C_1, C_2, \cdots, C_n$, deren eigentliche Anzahl wegen (33) nur $s = r + q$ beträgt, falls $s \overline{>} 2$ ist, alle bis auf eine nach Belieben, also, indem man sie als rationale Brüche wählt, als nicht algebraisch ganze Zahlen voraussetzen, und so erweist sich dann auch dieser zweite Fall als unzulässig. Ist dagegen $s = 1$, was, abgesehen vom Körper der rationalen Zahlen, nur sein kann, wenn $n = 2$ ist, so haben wir im fünften Kapitel gesehen, daß die Grundzahl eines quadratischen Körpers immer von ± 1 verschieden ist, und der zu begründende Satz ist hierdurch aufs neue völlig erwiesen.

Zum Beweise endlich des zweiten oben ausgesprochenen Satzes denke man sich alle Körper n^{ten} Grades mit der Grundzahl D und setze $\varDelta = |\sqrt{D}|$. Ist $\mathfrak{K}$ einer dieser Körper, so nehme man die n Konjugierten $\mathfrak{K}^{(1)}, \mathfrak{K}^{(2)}, \cdots, \mathfrak{K}^{(n)}$ und wähle, falls $\mathfrak{K}$ reell ist, $\mathfrak{K}^{(1)} = \mathfrak{K}$ und $C_1 = \varDelta^{\frac{n-1}{n}}$, alle übrigen Konstanten $C_i = \varDelta^{-\frac{1}{n}}$; andernfalls $\mathfrak{K}^{(r+1)} = \mathfrak{K}$ und $C_{r+1} = C_{r+q+1} = \varDelta^{\frac{n-2}{2n}}$, alle übrigen Konstanten $C_i = \varDelta^{-\frac{1}{n}}$, eine Wahl dieser Konstanten, die sich mit den Bedingungen (33), (34) offenbar verträgt. Nach dem letzten Satze voriger Nummer ist ein System nicht verschwindender ganzer Zahlen u_i vorhanden, für welches die im absoluten Sinne zu nehmenden Ungleichheiten bestehen:

im ersten Falle

$$\mathfrak{f}_1 \overline{<} \varDelta, \quad \text{für } i > 1 \text{ aber } \mathfrak{f}_i < 1,$$

im zweiten Falle

$$\mathfrak{f}_{r+1} < \varDelta^{\frac{1}{2}}, \ \mathfrak{f}_{r+q+1} < \varDelta^{\frac{1}{2}}, \text{ für die übrigen } i \text{ aber } \mathfrak{f}_i < 1.$$

Daraus ergibt sich aber in beiden Fällen erstens, daß die absoluten Beträge der ganzen Zahlen $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$, welche jenen ganzzahligen Systemen der Unbestimmten zugehören, unterhalb endlicher Grenzen liegen und es folglich nach dem

Hilfssatze in Nr. 4 des 4. Kapitels nur eine endliche Anzahl ganzer algebraischer Zahlen gibt, welche den Ungleichheiten genügen; zweitens, daß die Zahl $w^{(1)}$ bezw. $w^{(r+1)}$ des betrachteten Körpers, da $N(w) > 1$, sich von allen ihren Konjugierten unterscheidet, demnach ihre Differente nicht Null und sie selbst eine erzeugende Zahl des Körpers ist. Da es hiernach für jeden der Körper n^{ten} Grades mit der Grundzahl D eine ihn erzeugende Zahl gibt, welche sich unter der bezeichneten endlichen Menge ganzer Zahlen befinden muß, so kann auch die Anzahl jener Körper nur eine endliche sein, wie behauptet. (Vgl. Hilberts Bericht p. 213).

8. Kehren wir nach dieser Abschweifung zur Betrachtung der Einheiten wieder zurück, um das in Nr. 4 erhaltene Resultat aus dem allgemeinen Minkowskischen Satze herzuleiten (vgl. Hilberts Bericht, p. 216). Indem wir uns wieder auf eine bestimmte Ordnung $\mathfrak{o}$ des Körpers beschränken, geben wir den Zeichen wieder die gleiche Bedeutung wie in Nr. 2. Wir beweisen dann zunächst folgenden Satz:

Es gibt in $\mathfrak{o}$ eine Einheit ε mit positiver Norm, für welche der mit beliebigen, nicht sämtlich verschwindenden reellen Konstanten $g_1, g_2, \cdots, g_{s-1}$ gebildete Ausdruck

$$g_1 l_1(\varepsilon) + g_2 l_2(\varepsilon) + \cdots + g_{s-1} l_{s-1}(\varepsilon) \tag{40}$$

positiv ist. Behufs des Beweises setzen wir zur Abkürzung für irgend eine von Null verschiedene Zahl ω in $\mathfrak{o}$

$$L(\omega) = g_1 l_1(\omega) + g_2 l_2(\omega) + \cdots + g_{s-1} l_{s-1}(\omega) \tag{41}$$

und wählen $s-1$ reelle Größen $h_1, h_2, \cdots, h_{s-1}$ so, daß

$$h_1 g_1 + h_2 g_2 + \cdots + h_{s-1} g_{s-1} = 1 \tag{42}$$

wird. Ferner setzen wir, falls sämtliche n zu einander konjugierte Körper reell sind,

$$k_1 = e^{h_1 u},\ k_2 = e^{h_2 u},\ \cdots,\ k_{n-1} = e^{h_{n-1} u}, \qquad k_n = \frac{\Delta}{k_1 k_2 \cdots k_{n-1}}, \tag{43^a}$$

wo u einen beliebigen reellen Wert bezeichnet, entgegengesetztenfalls aber

(43ᵇ) $$k_1 = e^{h_1 u}, \cdots, k_r = e^{h_r u}, k_{r+1} = e^{h_{r+1} \cdot \frac{u}{2}}, \cdots,$$
$$k_{r+q-1} = e^{h_{r+q-1} \cdot \frac{u}{2}}$$
$$k_{r+q} = \sqrt{\frac{\Delta}{k_1 \cdots k_r k_{r+1}^2 \cdots k_{r+q-1}^2}}$$

und ferner allgemein $k_{r+i} = k_{r+q+i}$ für $i = 1, 2, \cdots, q$. Bei dieser Wahl der Konstanten k_i findet sich offenbar die Gleichung

(44) $$k_1 k_2 \cdots k_n = \Delta$$

und somit alle Voraussetzungen des Minkowskischen Satzes in seiner zweiten Fassung für die n linearen Formen (8ᵃ) erfüllt. Demnach kann in ihnen für die Unbestimmten u_i ein System nicht verschwindender ganzer Zahlen gesetzt werden, so, daß die Ungleichheiten

(45) $$|\mathfrak{f}_i| \leqq k_i$$

befriedigt sind. Hieraus folgt für das entsprechende Produkt (38) oder für die Norm der den gedachten ganzzahligen Werten der Unbestimmten zugehörigen Zahl ω der Ordnung die Ungleichheit

(46) $$N(\omega) \leqq \Delta.$$

Da jedoch $N(\omega)$ stets $\geqq 1$ ist, so ist für jeden Index i

(47) $$|\omega^{(i)}| \geqq \left| \frac{1}{\omega^{(1)} \cdots \omega^{(i-1)} \cdot \omega^{(i+1)} \cdots \omega^{(n)}} \right|,$$

und da aus (45) allgemein auch

$$|\omega^{(i)}| \leqq k_i$$

zu schließen ist, so ergibt sich mit Beachtung von (44) aus (47) die neue Ungleichheit

$$|\omega^{(i)}| \geqq \frac{k_i}{\Delta},$$

die mit der vorigen verbunden und in Beachtung der Bestimmungen (43ᵃ), (43ᵇ) durch den Übergang zu den Logarithmen die folgenden erschließen läßt:

$$h_i u \gtreqless l_i(\omega) \gtreqless h_i u - c_i\delta \gtreqless h_i u - 2\delta,$$
$$(i = 1, 2, \cdots, s-1)$$

in denen δ den reellen Bestandteil von $\log \varDelta$ bedeutet. Ihnen zufolge bleibt für jeden Index i aus der Reihe $1, 2, \cdots, s-1$ der absolute Wert des Unterschiedes

$$l_i(\omega) - h_i u$$

zwischen den Grenzen 0 und 2δ, woraus dann folgt, daß auch der Ausdruck

$$L(\omega) - u$$
$$= g_1(l_1(\omega) - h_1 u) + g_2(l_2(\omega) - h_2 u) + \cdots + g_{s-1}(l_{s-1}(\omega) - h_{s-1} u),$$

welchen Wert die reelle Größe u auch habe, zwischen zwei Grenzen δ' und $\delta'' > \delta'$ enthalten bleiben muß, die nicht von diesem Werte von u, sondern lediglich von der Grundzahl des Körpers und von den Konstanten g_i bestimmt sind. Setzt man nun $d = \delta'' - \delta'$ und successive

$$u = 0,\ u = d,\ u = 2d,\ \cdots,$$

so entspringen aus dem vorigen Verfahren für diese besonderen Werte für u unbegrenzt viele Zahlen $\omega^0, \omega', \omega'', \cdots$ der Ordnung, deren Normen wegen (46) absolut genommen nicht größer als $\varDelta$ sein können, während

$$L(\omega^0),\ L(\omega') - d,\ L(\omega'') - 2d,\ \cdots$$

sämtlich zwischen δ' und δ'' enthalten sind, sodaß die Werte

$$L(\omega^0),\ L(\omega'),\ L(\omega''),\ \cdots$$

zwischen

$$\delta',\ \delta'';\ \delta'',\ 2\delta'' - \delta';\ 2\delta'' - \delta',\ 3\delta'' - 2\delta';\ \cdots$$

resp. liegen, also eine Reihe stets wachsender Werte bilden. Da jede Norm gleich einer rationalen ganzen Zahl, zwischen $\pm \varDelta$ aber nur eine endliche Menge solcher Zahlen vorhanden ist, müssen unendlich viele der Zahlen $\omega^0, \omega', \omega'', \cdots$ ein- und dieselbe Norm N besitzen und unter den letzteren wieder (vgl. Nr. 3) mindestens zwei vorhanden sein — wir nennen die frühere derselben λ, die spätere μ — deren ganzzahlige Koeffizienten (mod. N) kongruent sind, derart, daß

$$\mu - \lambda = N \cdot \omega$$

ist, unter ω eine Zahl der Ordnung verstanden. Hieraus folgt

nun, wie in Nr. 3, die Existenz einer Einheit $\varepsilon = \frac{\mu}{\lambda}$ mit positiver Norm in der Ordnung von der Beschaffenheit, daß

$$L(\mu) - L(\lambda)$$
$$= g_1 l_1\left(\frac{\mu}{\lambda}\right) + g_2 l_2\left(\frac{\mu}{\lambda}\right) + \cdots + g_{s-1} l_{s-1}\left(\frac{\mu}{\lambda}\right) > 0$$

oder der Ausdruck (40) positiv ausfällt, womit die Behauptung des Satzes erwiesen ist.

Mit Hilfe dieses Ergebnisses, welches durch den in Nr. 3 hergeleiteten *Dirichlet*schen Satz nur bestätigt wird, läßt sich nun aber der der Nr. 4 sogleich wieder gewinnen. Wählt man nämlich die Konstanten

$$g_1 = 1, \text{ für } i > 1 \text{ aber } g_i = 0,$$

so gibt es dem letzten Ergebnisse zufolge in $\mathfrak{o}$ eine Einheit ε_1 mit positiver Norm, für welche l_{11} positiv ist. Sind ferner schon — unter m eine Zahl $< s$ verstanden — $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{m-1}$ $m-1$ Einheiten der Ordnung mit positiver Norm, für welche die in Nr. 4 mit L' bezeichnete Determinante positiv ist, und wählt man für die Konstanten g_i die Werte

$$g_1 = A_1, \; g_2 = A_2, \; \cdots, \; g_m = A_m, \text{ für } i > m \text{ aber } g_i = 0,$$

unter denen wenigstens der eine Wert für g_m nicht verschwindet, da er gleich L' ist, so folgt aus dem Bewiesenen die Existenz einer Einheit ε_m in $\mathfrak{o}$ mit positiver Norm von der Beschaffenheit, daß auch die dort mit L'' bezeichnete Determinante positiv ausfällt, und da dieser Schluß bis $m = s-1$ hin gezogen werden kann, so ergibt sich schließlich der Dirichletsche Satz.

9. Bei der weiteren Darstellung der Dirichletschen Theorie kann man nun nach Belieben sich auf diejenigen Einheiten der Ordnung beschränken, deren Normen positiv sind, oder ihre sämtlichen Einheiten in Betracht ziehen. Im Ausspruche der einzelnen Sätze werden wir diesem doppelten Gesichtspunkte Rechnung tragen, indem wir, was auf den beschränkteren Bezug hat, in Parenthesen setzen.

Ausgehend von dem Systeme S von $s-1$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ mit positiver Norm, deren Existenz

auf mehrfache Weise nachgewiesen worden ist, wollen wir vor allem die Beziehung bemerken, welche folgt:

$$(48)\qquad \begin{vmatrix} l_{11}, & l_{12}, & \cdots, l_{1,s-1}, & u_1 \\ l_{21}, & l_{22}, & \cdots, l_{2,s-1}, & u_2 \\ \cdot & \cdot & \cdot & \cdot \\ l_{s-1,1} & l_{s-1,2}, & \cdots, l_{s-1,s-1}, & u_{s-1} \\ l_{s1}, & l_{s2}, & \cdots, l_{s,s-1}, & u_s \end{vmatrix} = L\cdot(u_1+u_2+\cdots+u_s),$$

und in welcher L die Determinante (24) bezeichnet. In der Tat gehen von den Gliedern in der letzten Horizontalreihe der s-gliedrigen Determinante, indem man, was die Determinante selbst nicht verändert, diejenigen der früheren Reihen zu ihnen addiert, die ersten $s-1$ in

$$l_{1i}+l_{2i}+\cdots+l_{s-1,i}+l_{si}=0$$

(nach (22)), das letzte in

$$u_1+u_2+\cdots+u_{s-1}+u_s$$

über, woraus dann die Gleichung (48) sogleich erhellt. Mit Rücksicht auf die Beziehung (20) erschließt man folglich die Gleichung

$$(49)\qquad \begin{vmatrix} l_{11}, & l_{12}, & \cdots, l_{1,s-1}, & c_1 \\ \cdot & \cdot & \cdot & \cdot \\ l_{s-1,1}, & l_{s-1,2}, & \cdots, l_{s-1,s-1}, & c_{s-1} \\ l_{s1}, & l_{s2}, & \cdots, l_{s,s-1}, & c_s \end{vmatrix} = nL,$$

welche lehrt, daß diese Determinante einen nicht verschwindenden, nämlich positiven Wert hat.

Bedeutet daher ω irgend eine Zahl der Ordnung $\mathfrak{o}$, so lassen sich reelle Werte $e_1, e_2, \cdots, e_{s-1}, f$ auf eindeutige Weise so bestimmen, daß die folgenden Gleichungen erfüllt sind:

$$(50)\qquad \begin{cases} e_1\cdot l_{11} + e_2\cdot l_{12} + \cdots + e_{s-1}\cdot l_{1,s-1} + f\cdot c_1 = l_1(\omega) \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ e_1\cdot l_{s-1,1} + e_2\cdot l_{s-1,2} + \cdots + e_{s-1}\cdot l_{s-1,s-1} + f\cdot c_{s-1} = l_{s-1}(\omega) \\ e_1\cdot l_{s1} + e_2\cdot l_{s2} + \cdots + e_{s-1}\cdot l_{s,s-1} + f\cdot c_s = l_s(\omega). \end{cases}$$

Die mit ω veränderlichen, also als Funktionen von ω aufzufassenden Werte $e_1, e_2, \cdots, e_{s-1}, f$ oder

$$e_1(\omega),\ e_2(\omega),\ \cdots,\ e_{s-1}(\omega),\ f(\omega),$$

deren $s-1$ ersten die Exponenten für ω heißen mögen,

haben zufolge der Beziehung (23) offenbar die Eigenschaft, daß für zwei beliebige Zahlen α, β der Ordnung

$$(51)\quad \begin{cases} e_i(\alpha\beta) = e_i(\alpha) + e_i(\beta), & (\text{für } i = 1, 2, \cdots, s-1) \\ f(\alpha\beta) = f(\alpha) + f(\beta) \end{cases}$$

ist. Durch Addition der Gleichungen (50) erkennt man ferner sogleich die Bedeutung der Größe $f(\omega)$, indem so folgende Beziehung:

$$(52)\quad n \cdot f(\omega) = \log |N(\omega)|$$

hervorgeht. Aus ihr findet sich insbesondere für den Fall, daß ω eine beliebige Einheit ε in $\mathfrak{o}$ ist, gleichviel, ob deren Norm $+1$ oder -1 ist,

$$(53)\quad f(\varepsilon) = 0.$$

Bildet man daher mittels der $s-1$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ (mit positiver Norm) und $s-1$ beliebigen, positiven oder negativen ganzen Zahlen $m_1, m_2, \cdots, m_{s-1}$, die Null inklusive, den Ausdruck

$$(54)\quad \varepsilon = \varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_{s-1}^{m_{s-1}},$$

welcher nach der Vorbemerkung in Nr. 2 eine Einheit in $\mathfrak{o}$ (mit positiver Norm) ist, und aus welchem die Gleichungen

$$\begin{aligned} m_1 \cdot l_{11} + m_2 \cdot l_{12} + \cdots + m_{s-1} \cdot l_{1,s-1} &= l_1(\varepsilon) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ m_1 \cdot l_{s-1,1} + m_2 \cdot l_{s-1,2} + \cdots + m_{s-1} \cdot l_{s-1,s-1} &= l_{s-1}(\varepsilon) \end{aligned}$$

hervorgehen, so ergibt die Vergleichung der letzteren mit den aus (50) entspringenden:

$$\begin{aligned} e_1 \cdot l_{11} + e_2 \cdot l_{12} + \cdots + e_{s-1} \cdot l_{1,s-1} &= l_1(\varepsilon) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ e_1 \cdot l_{s-1,1} + e_2 \cdot l_{s-1,2} + \cdots + e_{s-1} \cdot l_{s-1,s-1} &= l_{s-1}(\varepsilon) \end{aligned}$$

wegen der Eindeutigkeit der Gleichungen (50) die folgenden Formeln:

$$m_i = e_i, \quad (i = 1, 2, \cdots, s-1)$$

welche lehren, daß die Exponenten im Ausdrucke (54) eindeutig bestimmt sind, oder daß dieselbe Einheit ε nicht auch noch durch die Formel

$$\varepsilon = \varepsilon_1^{n_1} \varepsilon_2^{n_2} \cdots \varepsilon_{s-1}^{n_{s-1}}$$

gegeben werden kann, wenn nicht die Exponenten n_i sämtlich mit den m_i identisch sind. Hieraus folgt, daß die Formel (54), wenn man darin die Exponenten m_i sämtliche ganze Zahlen durchlaufen läßt, einen Komplex von lauter verschiedenen, unendlich vielen Einheiten der Ordnung (mit positiver Norm) liefert.

Demnach bezeichnet der Ausdruck

$$\omega = \omega_0 \cdot \varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_{s-1}^{m_{s-1}}, \tag{55}$$

wenn ω_0 irgend eine bestimmte Zahl der Ordnung bedeutet, ebenfalls einen Komplex von unendlich vielen, voneinander verschiedenen Zahlen der Ordnung. Nun seien in den auf ω_0 bezüglichen mit (50) analogen Gleichungen die größten in den zugehörigen „Exponenten“ e_i enthaltenen Ganzen die Zahlen n_i, und b_i die übrig bleibenden Bruchteile, sodaß

$$e_i = n_i + b_i, \quad 0 \overline{\gtrless} b_i < 1$$
$$(i = 1, 2, \cdots, s-1)$$

zu setzen ist. Dann findet sich das folgende System von Gleichungen:

$$l_i(\omega_0) = (n_1 + b_1) l_{i1} + \cdots + (n_{s-1} + b_{s-1}) l_{i,s-1} + f c_s,$$
$$(i = 1, 2, \cdots, s-1)$$

während aus (55) dies andere:

$$l_i(\omega) = l_i(\omega_0) + m_1 l_{i1} + \cdots + m_{s-1} l_{i,s-1}$$
$$(i = 1, 2, \cdots, s-1)$$

oder:

$$l_i(\omega) = (n_1 + b_1 + m_1) l_{i1} + \cdots + (n_{s-1} + b_{s-1} + m_{s-1}) l_{i,s-1} + f c_s$$
$$(i = 1, 2, \cdots, s-1)$$

hervorgeht. Ihm zufolge können die ganzzahligen Exponenten m_i auf eindeutig bestimmte Weise so gewählt werden, daß die Koeffizienten der Größen l_{ik} sämtlich zwischen 0 und 1 fallen, die Null inklusive; man hat zu diesem Zwecke offenbar nur die m_i den durch ω_0 völlig bestimmten Zahlen n_i entgegen zu setzen:

$$m_i = -n_i.$$

So erkennt man, daß in jedem Komplexe (55) ein einziges Glied ω vorhanden ist, dessen Exponenten in den bezüglichen mit (50) analogen Gleichungen zwischen 0 und 1 liegen. Nennt man jede Zahl der Ordnung, deren Exponenten diese

Eigenschaft haben, eine reduzierte Zahl derselben, so folgt also der Ausspruch:

In jedem Komplexe liegt eine einzige reduzierte Zahl.

Ferner gilt aber der allgemeine Satz, der uns später von wesentlichem Nutzen sein wird: Es gibt nur eine endliche Anzahl reduzierter Zahlen ω der Ordnung, deren Norm absolut nicht größer ist als eine gegebene Zahl z. Da nämlich dann in den bezüglichen Gleichungen (50) sowohl die Exponenten e_i die endliche Grenze 1, als auch wegen (52) die Zahl f die endliche Grenze $\frac{\log z}{n}$ nicht überschreiten, so verbleiben auch die sämtlichen Werte

$$l_1(\omega),\ l_2(\omega),\ \cdots,\ l_s(\omega),$$

desgleichen also auch die Potenzen

$$e^{\frac{l_1(\omega)}{c_1}},\ e^{\frac{l_2(\omega)}{c_2}},\ \cdots,\ e^{\frac{l_s(\omega)}{c_s}},$$

d. i. die absoluten Beträge der Konjugierten $\omega^{(i)}$ innerhalb endlicher Grenzen, woraus nach Kap. 4, Nr. 4 folgt, daß die Anzahl solcher Zahlen ω nur eine endliche ist.

Hiernach gibt es also in der Ordnung auch nur eine endliche Anzahl reduzierter *Einheiten* (umsomehr also auch nur eine endliche Anzahl solcher Einheiten mit positiver Norm); sie mögen durch

$$\eta_0,\ \eta_1,\ \eta_2,\ \cdots,\ \eta_{\varrho-1} \tag{56}$$

bezeichnet werden. Ihnen entsprechen ϱ Komplexe von Einheiten (mit positiver Norm):

$$\eta_i \cdot \varepsilon_1^{m_1}\varepsilon_2^{m_2}\cdots\varepsilon_{s-1}^{m_{s-1}}, \quad (i = 0, 1, 2, \cdots, \varrho - 1) \tag{57}$$

deren je zwei durchweg voneinander verschieden sein müssen; denn, wären etwa zwei Ausdrücke

$$\eta_i \cdot \varepsilon_1^{m_1}\varepsilon_2^{m_2}\cdots\varepsilon_{s-1}^{m_{s-1}},\quad \eta_k \cdot \varepsilon_1^{n_1}\varepsilon_2^{n_2}\cdots\varepsilon_{s-1}^{n_{s-1}}$$

einander gleich, so ergäbe sich offenbar η_k als eine Zahl des η_i entsprechenden Komplexes, der dann zwei reduzierte Zahlen η_i, η_k enthielte, was nicht sein kann. Da andererseits aus jeder beliebigen Einheit η der Ordnung (mit positiver Norm) ein Komplex gebildet werden kann, der eine reduzierte Zahl

d. i. eine der Zahlen (56) enthält, und η folglich umgekehrt in dem aus dieser gebildeten Komplexe enthalten sein muß, so leuchtet ein, daß sämtliche Einheiten der Ordnung (mit positiver Norm) und jede von ihnen auch nur einmal durch die ϱ Komplexe (57) geliefert werden müssen, indem man darin die Exponenten m_i alle positiven und negativen ganzen Zahlen durchlaufen läßt.

Aus diesem Ergebnisse folgert man leicht den Umstand, daß für jede Einheit ε der Ordnung (mit positiver Norm) die Potenz ε^ϱ von der Form

$$\varepsilon_1^{m_1}\varepsilon_2^{m_2}\cdots\varepsilon_{s-1}^{m_{s-1}} \tag{58}$$

mit ganzzahligen Exponenten ist. Denn gewiß werden die ϱ Einheiten

$$\varepsilon\eta_0,\ \varepsilon\eta_1,\ \cdots,\ \varepsilon\eta_{\varrho-1}$$

je einem der ϱ Komplexe (57) angehören, mithin wird, wenn $\eta_0', \eta_1', \cdots, \eta_{\varrho-1}'$ Einheiten der Reihe (56) und $\varepsilon^{(0)}, \varepsilon^{(1)} \cdots, \varepsilon^{(\varrho-1)}$ Produkte von der Form (58) bedeuten,

$$\varepsilon\eta_0 = \eta_0'\cdot\varepsilon^{(0)},\ \varepsilon\eta_1 = \eta_1'\cdot\varepsilon^{(1)},\ \cdots,\ \varepsilon\eta_{\varrho-1} = \eta_{\varrho-1}'\cdot\varepsilon^{(\varrho-1)}$$

gesetzt werden können. Hieraus folgt zunächst die Verschiedenheit der Einheiten $\eta_0', \eta_1', \cdots, \eta_{\varrho-1}'$ und folglich die Übereinstimmung ihrer Gesamtheit mit der Reihe (56), da z. B., wenn $\eta_0' = \eta_1'$ wäre, sich $\eta_0\varepsilon^{(1)} = \eta_1\varepsilon^{(0)}$ ergäbe, die reduzierten Einheiten η_0, η_1 also ein- und demselben Komplexe angehörten. Demnach ergeben die voraufgehenden Gleichungen ferner durch Multiplikation die folgende:

$$\varepsilon^\varrho = \varepsilon^{(0)}\varepsilon^{(1)}\cdots\varepsilon^{(\varrho-1)},$$

welche die Behauptung erweist. Und somit dürfen wir schließlich als das Endergebnis dieser Betrachtungen den Ausspruch tun:

Jede Einheit ε der Ordnung (mit positiver Norm) kann mittels eines Systems S von $s-1$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ mit positiver Norm in der Form

$$\varepsilon = \varepsilon_1^{\frac{m_1}{\varrho}}\cdot\varepsilon_2^{\frac{m_2}{\varrho}}\cdots\varepsilon_{s-1}^{\frac{m_{s-1}}{\varrho}} \tag{59}$$

dargestellt werden, in welcher die Exponenten rationale Zahlen, ihr gemeinsamer Nenner ϱ die Anzahl der bezüglich jenes Systems reduzierten Einheiten (mit positiver Norm) bezeichnen.

10. Man bemerke, daß, was in diesem Ausspruche angedeutet worden, der **Begriff der reduzierten Einheiten nur ein relativer**, nämlich auf das System S der $s-1$ unabhängigen Einheiten, welches der Betrachtung zum Grunde liegt, bezüglich ist; deshalb wird auch ihre Anzahl ϱ wechseln, wenn man statt **eines** solchen Systems ein **anderes** wählt. **Es gibt deren aber unendlich viele.** In der Tat, seien $E_1, E_2, \cdots, E_{s-1}$ irgend welche $s-1$ Einheiten der Ordnung (mit positiver Norm). Der Beziehung (59) zufolge bestehen für jede derselben $s-1$ Gleichungen:

$$l_k(E_i) = \frac{m_1^{(i)}}{\varrho}\, l_{k1} + \frac{m_2^{(i)}}{\varrho}\, l_{k2} + \cdots + \frac{m_{s-1}^{(i)}}{\varrho}\, l_{k,s-1}, \qquad (k = 1, 2, \cdots, s-1) \tag{60}$$

worin die Koeffizienten $m_1^{(i)}, m_2^{(i)}, \cdots, m_{s-1}^{(i)}$ rationale ganze Zahlen sind. Aus diesen $s-1$ Systemen von je $s-1$ Gleichungen ergibt sich aber die folgende Beziehung zwischen der Determinante L und der analog mit ihr aus den Einheiten E_i gebildeten Determinante L:

$$\mathrm{L} = \frac{M}{\varrho^{s-1}} \cdot L, \tag{61}$$

wenn man mit M die aus den Koeffizienten $m_k^{(i)}$ gebildete Determinante bezeichnet. Hieraus folgt, daß das System von $s-1$ Einheiten $E_1, E_2, \cdots, E_{s-1}$ (mit positiver Norm) dann und nur dann ebenso wie dasjenige der $s-1$ Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ ein unabhängiges, d. h. seine Determinante L positiv sein wird, wenn die Determinante M positiv ist. Es ist aber ersichtlich, daß es unendlich viel Einheitssysteme $E_1, E_2, \cdots, E_{s-1}$ geben wird, für welche dies geschieht; denn, wählt man die $m_k^{(i)}$ als beliebige Vielfache von ϱ, so werden die E_i Glieder des Komplexes (54), also Einheiten der Ordnung (mit positiver Norm) sein und die Vielfachen offenbar auf unendlich viel Weisen so gewählt werden können, daß M einen von Null verschiedenen, positiven Wert erhält. Nun ist M stets eine **ganze** Zahl. Unter allen zulässigen Systemen der $m_k^{(i)}$ wird demnach mindestens eins angebbar sein, für welches M den **kleinsten** Wert m erhält und damit auch L ein Minimum wird. Das zugehörige System von $s-1$ Einheiten

$E_1, E_2, \cdots, E_{s-1}$ heiße ein Fundamentalsystem von Einheiten der Ordnung.

Wählt man dieses System an Stelle des bisherigen Systems S, womit dann L die auf das Fundamentalsystem $E_1, E_2, \cdots, E_{s-1}$ bezügliche Determinante vom kleinsten Werte wird, so gelten die analogen Resultate, insbesondere gibt es nur eine endliche Anzahl bezüglicher reduzierter Einheiten (mit positiver Norm), welche wieder mit ϱ, sie selbst mit

$$H_0, H_1, \cdots, H_{\varrho-1}$$

bezeichnet werden mögen, und sämtliche Einheiten der Ordnung (mit positiver Norm) werden erhalten, und jede von ihnen auch nur einmal, aus den ϱ Komplexen

$$H_i \cdot E_1^{m_1} E_2^{m_2} \cdots E_{s-1}^{m_{s-1}}, \quad (i = 0, 1, 2, \cdots, \varrho - 1) \tag{62}$$

wenn man darin die Exponenten m_i alle rationalen ganzen Zahlen durchlaufen läßt.

Aber für ein Fundamentalsystem kommt den reduzierten Einheiten eine ausgezeichnete Eigenschaft zu: sie sind die sämtlichen Wurzeln der Gleichung

$$x^\varrho = 1. \tag{63}$$

Für jede der Einheiten H_i nämlich müssen sämtliche zugehörige Exponenten $e_1, e_2, \cdots, e_{s-1}$ gleich Null sein. Denn, wählt man statt des Systems der Einheiten $E_1, E_2, \cdots, E_{s-1}$ das System $H_i, E_2, \cdots, E_{s-1}$, so nehmen die $s-1$ Gleichungssysteme (60) die besondere Gestalt an:

$$l_k(H_i) = e_1 \cdot l_k(E_1) + e_2 \cdot l_k(E_2) + \cdots + e_{s-1} \cdot l_k(E_{s-1})$$
$$(k = 1, 2, \cdots, s-1)$$

$$l_k(E_h) = l_k(E_h) \qquad (h = 2, 3, \cdots, s-1),$$
$$(k = 1, 2, \cdots, s-1)$$

woraus für die Gleichung (61) die Gestalt

$$\mathrm{L} = e_1 \cdot L$$

hervorgeht, während e_1, wenn es nicht Null ist, einen positiven echten Bruch bedeutet; mithin wäre dann für jenes System von $s-1$ Einheiten die bezügliche Determinante L kleiner als die dem Fundamentalsysteme entsprechende Determinante L,

was nicht sein kann. Man schließt also e_1 und analog $e_2, \cdots, e_{s-1}$ gleich Null, mithin verschwinden sämtliche Logarithmen $l_k(H_i)$.

Eine Einheit aber (mit positiver Norm), deren sämtliche Logarithmen verschwinden, ist eine ϱ^{te} Einheitswurzel.[1]) In der Tat folgt aus dem Schlußsatze der vorigen Nummer für jede Einheit E der Ordnung (mit positiver Norm) eine Gleichung von der Form:

$$E^\varrho = E_1^{m_1} E_2^{m_2} \cdots E_{s-1}^{m_{s-1}}$$

mit ganzzahligen Exponenten m_i, woraus, wenn die sämtlichen Logarithmen $l_k(E) = 0$ sind, sich $s-1$ Gleichungen

$$0 = m_1 l_k(E_1) + m_2 l_k(E_2) + \cdots + m_{s-1} l_k(E_{s-1})$$
$$(k = 1, 2, \cdots, s-1)$$

mit nicht verschwindender Determinante, folglich die Werte $m_i = 0$ und somit

$$E^\varrho = 1$$

ergibt. Hiernach ist in der Tat jede der ϱ reduzierten Einheiten H_i eine Wurzel der Gleichung (63), und, da es ϱ verschiedene solcher Einheiten gibt, machen sie die Gesamtheit dieser Wurzeln aus. — Andererseits ist offenbar jede in $\mathfrak{o}$ enthaltene Einheitswurzel η (für welche $N(\eta) > 0$ ist) eine Einheit der Ordnung (mit positiver Norm), deren sämtliche Logarithmen Null sind; also stimmt die Gesamtheit der reduzierten Einheiten H_i mit der Gesamtheit aller in $\mathfrak{o}$ enthaltenen Einheitswurzeln (der angegebenen Art) überein.

Auf solche Weise ist schließlich der folgende Dirichletsche Hauptsatz über die Einheiten festgestellt:

Alle Einheiten einer Ordnung (mit positiver Norm) werden durch die Formel

$$E = H \cdot E_1^{m_1} E_2^{m_2} \cdots E_{s-1}^{m_{s-1}}, \tag{64}$$

in welcher $E_1, E_2, \cdots, E_{s-1}$ ein System fundamentaler Einheiten der Ordnung mit positiver Norm, d. i. ein solches System von $s-1$ Einheiten mit positiver Norm bezeichnen, deren zugehörige Determinante

$$| \, l_k(E_i) \, | \tag{65}$$
$$(i, k = 1, 2, \cdots, s-1)$$

1) Vgl. Kronecker, zwei Sätze über Gleichungen mit ganzzahligen Koeffizienten, Werke I, p. 103, sowie Minkowski, Geometrie der Zahlen, p. 136.

den kleinstmöglichen positiven Wert hat, dadurch erhalten — und jede von ihnen auch nur einmal —, daß man die Exponenten m_i alle möglichen rationalen ganzen Zahlen, H aber die endliche Anzahl aller in der Ordnung enthaltenen Einheitswurzeln (für welche $N(H) > 0$ ist) durchlaufen läßt.

Nach Dedekind nennt man den Absolutwert der Determinante (65) den Regulator des Systems von Fundamentaleinheiten oder, da er von der willkürlichen Auswahl dieses Systems, wie leicht zu erkennen, unabhängig ist, den Regulator der Ordnung bezw. für $\mathfrak{o} = \mathfrak{g}$ des Körpers.

Indem man nun für die beliebige Ordnung $\mathfrak{o}$ die besondere Ordnung $\mathfrak{g}$ aller ganzen Zahlen des Körpers setzt, erhält man die Gesamtheit aller Einheiten des Körpers (mit positiver Norm) durch einen völlig entsprechenden Satz. Was in diesem Satze die reduzierten Einheiten betrifft, so muß man unterscheiden, ob man sämtliche Einheiten oder nur diejenigen Einheiten des Körpers, deren Norm $+1$ ist, ins Auge fassen will. Handelt es sich um *sämtliche* Einheiten, so sind stets die beiden Zahlen ± 1 Einheiten des Körpers, welche, da sie zugleich Einheitswurzeln sind, zu den Zahlen H zählen; weil sie als solche Wurzeln der Gleichung (63) sind, muß folglich ϱ, d. i. die Anzahl aller reduzierten Einheiten gerade sein. Man bedenke nun, daß aus den Einheiten des betrachteten Körpers diejenigen der konjugierten Körper erhalten werden, wenn in der Formel (64) für H und die E_i ihre Konjugierten gesetzt werden; da die H aber der ganzzahligen Gleichung (63) genügen, sind ihre Konjugierten gleichfalls Wurzeln derselben, demnach ist für jeden der konjugierten Körper die Gesamtheit der reduzierten Einheiten H oder der in ihnen vorhandenen Einheitswurzeln dieselbe. Daher kann ϱ nur größer als 2 sein, wenn $n = 2q$, denn für $\varrho > 2$ wären imaginäre Einheitswurzeln in jedem der konjugierten Körper vorhanden, keiner derselben also könnte reell und folglich müßte $r = 0$, d. i. $n = 2q$ sein. — Beschränkt man sich jedoch auf die Betrachtung derjenigen Einheiten des Körpers, deren Norm $+1$ ist, so wäre -1 nur dann als eine Einheit mitzuzählen, wenn n gerade ist, da sonst

$N(-1) = (-1)^n$ negativ wird. Während demnach, so oft n gerade ist, auch jetzt dasselbe gilt, wie bei der allgemeinen Auffassung, kann dagegen im Falle eines ungeraden n die Zahl ϱ nur ungerade und, da sie aus gleichen Gründen wie zuvor nicht größer als 2 sein kann, nur gleich 1 sein, und die einzige reduzierte Einheit ist dann selber gleich 1.

Noch eine Bemerkung, welche Minkowski gemacht hat[1]), müssen wir hier anschließen. Wir dürfen dabei wieder statt der Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen eine beliebige Ordnung $\mathfrak{o}$ des Körpers betrachten. Ist α eine bestimmte Zahl derselben, so gibt es in ihr dem Hilfssatze in Nr. 4 des 4. Kapitels zufolge nur eine endliche Anzahl Zahlen ω, für welche die absoluten Beträge der Konjugierten $\omega^{(i)}$ nicht größer sind als diejenigen der Konjugierten $\alpha^{(i)}$. Wählt man unter ihnen eine Zahl β, deren Konjugierten dem absoluten Betrage nach, wenn möglich, sämtlich kleiner sind als diejenigen von α, so ist die Anzahl derjenigen Zahlen, für welche die absoluten Beträge der Konjugierten wieder nicht größer sind, als diejenigen von $\beta^{(i)}$, sicherlich kleiner als die erstere Anzahl. Wird unter ihnen wieder, wenn möglich, eine Zahl γ gewählt, deren Konjugierten absolut kleiner sind als diejenigen von β, so wird aufs neue die Anzahl derjenigen Zahlen, für welche die absoluten Beträge der Konjugierten nicht größer sind als diejenigen von γ, wieder kleiner sein als die vorige, usw. So gelangt man, ausgehend von jeder beliebigen Zahl der Ordnung notwendig zu einer Zahl ν derselben von der Beschaffenheit, daß es keine von Null verschiedene Zahl ω in der Ordnung mehr gibt, für welche die sämtlichen Ungleichheiten

$$\omega^{(i)} \text{ absolut } < \nu^{(i)} \qquad (i = 1, 2, \cdots, n) \tag{66}$$

erfüllt sind. Jede solche Zahl ν soll eine niedrigste Zahl der Ordnung heißen. Ist aber ν eine solche Zahl und ε irgend eine Einheit in $\mathfrak{o}$, so ist auch $\nu\varepsilon$ eine niedrigste Zahl, denn, gäbe es eine Zahl ω in $\mathfrak{o}$, für welche

1) Minkowski, Geometrie der Zahlen, p. 145/146.

$$\omega^{(i)} \text{ absolut } < \nu^{(i)}\varepsilon^{(i)},$$
$$(i = 1, 2, \cdots, n)$$

so wäre $\frac{\omega}{\varepsilon}$ eine andere Zahl in $\mathfrak{o}$, für welche

$$\left(\frac{\omega}{\varepsilon}\right)^{(i)} \text{ absolut } < \nu^{(i)}$$
$$(i = 1, 2, \cdots, n)$$

entgegen der vorausgesetzten Eigenschaft von ν. Hiernach lassen sich alle niedrigsten Zahlen in Komplexe von der Form

$$\nu \cdot \varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_{s-1}^{m_{s-1}}$$

verteilen und aus jedem derselben eine einzige in bezug auf das System S der $s-1$ unabhängigen Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ reduzierte niedrigste Zahl ν_0 entnehmen der Art, daß in den auf solche Zahl $\omega = \nu_0$ bezüglichen Gleichungen (50) die sämtlichen Exponenten $e_1, e_2, \cdots, e_{s-1}$ positive echte Brüche, Null inklusive, sind. Nun gibt es nach Nr. 7, worin man jedoch jetzt unter $\omega_1, \omega_2, \cdots, \omega_n$ wieder eine Basis der Ordnung $\mathfrak{o}$ und unter Δ die Quadratwurzel aus ihrer Diskriminante zu verstehen hat, dem Minkowskischen Satze gemäß eine Zahl ω in $\mathfrak{o}$, für welche die dort betrachteten Formen $\mathfrak{f}_i$ die Ungleichheiten

$$|\mathfrak{f}_i| \overline{<} C_i \cdot \sqrt[n]{\Delta}$$
$$(i = 1, 2, \cdots, n)$$

erfüllen, oder deren Konjugierte diese Grenzen nicht überschreiten. Daher muß, wenn ν_0 eine reduzierte niedrigste Zahl der Ordnung ist, wenigstens für einen Wert des Index i

$$|\nu_0^{(i)}| \overline{<} |\omega^{(i)}| \overline{<} C_i \cdot \sqrt[n]{\Delta}$$

sein, da sonst für alle i im Gegenteil $|\omega^{(i)}| < |\nu_0^{(i)}|$ wäre, was der Definition von ν_0 als niedrigster Zahl widerstreitet. Wäre nun etwa $|\nu_0^{(s)}| \overline{<} C_s \cdot \sqrt[n]{\Delta}$, so würde auch $l_s(\nu_0)$ und nach der letzten der Gleichungen (50) somit auch f auf endliche Grenzen beschränkt, womit dann auch durch die übrigen jener Gleichungen die sämtlichen Größen $l_1(\nu_0), l_2(\nu_0), \cdots, l_{s-1}(\nu_0)$, d. h. die sämtlichen Konjugierten von ν_0 ihrem Absolutwerte nach in endliche Grenzen gebannt bleiben. Nach dem Hilfs-

satze in Nr. 4 des 4. Kapitels kann daher die Anzahl der reduzierten niedrigsten Zahlen nur eine endliche sein.

Indem man diese endliche Menge der reduzierten niedrigsten Zahlen bestimmt, findet man daraus mit Hilfe aller Einheiten der Ordnung auch die zugehörigen Komplexe, d. h. die sämtlichen niedrigsten Zahlen der Ordnung. Aber man kann auch umgekehrt durch die Gesamtheit aller niedrigsten Zahlen diejenige aller Einheiten der Ordnung ermitteln. Denn jede jener Zahlen ν ist einer der reduzierten niedrigsten Zahlen ν_0 assoziiert, und indem man für alle mit ν_0 assoziierten niedrigsten Zahlen ν den Quotienten $\frac{\nu}{\nu_0}$ bildet, gewinnt man sämtliche Einheiten der Ordnung. Minkowski bemerkt, daß die Lagrangesche Methode zur Auflösung der Pellschen Gleichung, d. i. zur Ermittlung der Einheiten eines quadratischen Körpers für den Fall $n = 2$, $q = 0$ in der Tat diesem Vorgehen entspricht und hat in Nr. 45 seiner „Geometrie der Zahlen" dies eingehend erörtert.

Neuntes Kapitel.

Ideale einer Ordnung und die Anzahl ihrer Klassen.[1])

1. Nachdem im vorigen Abschnitte die Einheiten für jede Ordnung in $\mathfrak{g}$ ermittelt worden sind, sollen jetzt diese Ordnungen selbst genauer untersucht, insbesondere erläutert werden, wie die Arithmetik der Ideale sich auf diese beschränkteren Zahlengebiete übertragen läßt. Nachdem dann die Äquivalenz für die Ideale der Ordnung und ihre Einteilung in Klassen begründet worden sein wird, soll die Anzahl dieser Klassen sowohl für die Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen des Körpers, wie für jede einzelne Ordnung desselben ermittelt und diese mit jener verglichen werden.

1) S. zu diesem Kapitel Dedekinds Festschrift zur Säkularfeier des Geburtstages von Carl Friedrich Gauß, Braunschweig 1877.

Unter einer „Ordnung $\mathfrak{o}$ in $\mathfrak{g}$“ verstanden wir jeden n-gliedrigen Modulus ganzer Zahlen des Körpers, welcher die Eigenschaften einer Ordnung hat, denen zufolge alle rationalen ganzen Zahlen in $\mathfrak{o}$ enthalten sind und

$$\mathfrak{o} \cdot \mathfrak{o} = \mathfrak{o}$$

ist. Den Führer derselben nennen wir wieder $\mathfrak{f}$; er ist ein Ideal des Körpers und jedes andere in $\mathfrak{o}$ enthaltene Ideal ist teilbar durch $\mathfrak{f}$, d. i. auch im Führer enthalten.

Zuvörderst mag noch eine andere Definition solcher Ordnung angemerkt werden. Sind $\theta, \eta, \cdots$ irgend welche ganze Zahlen des Körpers, deren Rationalitätsbereich denselben erfüllt, sodaß alle seine Zahlen als rationale ganzzahlige Funktionen von $\theta, \eta, \cdots$ darstellbar sind, so ist der zugehörige Integritätsbereich offenbar eine Ordnung, nämlich ein Modulus, der ersichtlich die rationalen ganzen Zahlen umfaßt und dessen Zahlen mit einander multipliziert wieder Zahlen desselben ergeben. Aber genauer ist er auch eine „Ordnung in $\mathfrak{g}$“. Sei nämlich

$$[\alpha_1, \alpha_2, \cdots, \alpha_m] \tag{1}$$

die irreduktible Form dieses Modulus; da jede Zahl des Körpers als eine rationale Funktion von $\theta, \eta, \cdots$ mit ganzzahligen Koeffizienten darstellbar ist, kann sie auch als ganze Funktion derselben mit rationalen Koeffizienten aufgefaßt werden und geht demnach, mit einer gewissen ganzen Zahl multipliziert, in eine Zahl des Modulus über. Somit bestehen auch für die Basiszahlen $\gamma_1, \gamma_2, \cdots, \gamma_n$ von $\mathfrak{g}$ ganzzahlige Gleichungen von der Form

$$k_i \gamma_i = a_{i1} \alpha_1 + a_{i2} \alpha_2 + \cdots + a_{im} \alpha_m, \quad (i = 1, 2, \cdots, n)$$

welche lehren, daß m, das nicht größer sein kann als n, auch nicht kleiner als n und folglich gleich n ist, da sonst eine ganzzahlige Beziehung zwischen den Basiszahlen γ_i hervorgehen würde. Der Modulus (1) ist also ein n-gliedriger Modulus ganzer Zahlen des Körpers mit den Eigenschaften einer Ordnung, d. i. eine „Ordnung in $\mathfrak{g}$“, wie behauptet. Man ersieht hieraus, daß die „Ordnung in $\mathfrak{g}$“ auch als Integritätsbereich

irgend welcher, den Körper erzeugender Zahlen definiert werden kann.

Nun kann man für eine beliebige Ordnung $\mathfrak{o}$ dieser Art den Idealbegriff völlig analog formulieren, wie er für die besondere Ordnung $\mathfrak{g}$ gefaßt worden ist: als einen in $\mathfrak{o}$ enthaltenen Modulus $\mathfrak{i}$ von der Beschaffenheit, daß

$$\mathfrak{o} \cdot \mathfrak{i} \succ \mathfrak{i}$$

ist, eine Beziehung, welche durch die Gleichheit

$$\mathfrak{o} \cdot \mathfrak{i} = \mathfrak{i} \tag{2}$$

ersetzt werden darf, da die Einheit in $\mathfrak{o}$ enthalten, mithin auch umgekehrt $\mathfrak{i} \succ \mathfrak{o} \cdot \mathfrak{i}$ ist. Ein solches Ideal $\mathfrak{i}$ soll zum Unterschiede von den früher definierten Idealen des Körpers oder der besonderen Ordnung $\mathfrak{g}$ ein Ideal in $\mathfrak{o}$ oder der Ordnung $\mathfrak{o}$ genannt werden. Hilbert, welcher statt des Wortes „Ordnung" den Ausdruck „Ring" gebraucht, nennt dementsprechend solche Ideale „Ringideale".

Jedes Ideal $\mathfrak{i}$ in $\mathfrak{o}$ ist ein n-gliedriger Modulus. Sind nämlich $\omega_1, \omega_2, \cdots, \omega_n$ die Basiszahlen der Ordnung $\mathfrak{o}$ und α irgend eine von Null verschiedene Zahl des Ideales, so sind

$$\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_n \tag{3}$$

n rational unabhängige ganze Zahlen des Körpers, welche aber der Definition eines Ideales der Ordnung $\mathfrak{o}$ zufolge auch Zahlen des Ideals $\mathfrak{i}$ sind. Demnach kann jede Zahl des Körpers, insbesondere also auch jede Zahl der Ordnung $\mathfrak{o}$ mit einer rationalen ganzen Zahl multipliziert als eine ganzzahlige lineare Funktion der Zahlen (3), d. i. als eine Zahl in $\mathfrak{i}$ dargestellt werden. Da nun offenbar

$$\mathfrak{o} - \mathfrak{i} = \mathfrak{i}$$

ist, schließt man aus dem Hauptsatze der letzten Nummer des zweiten Kapitels, daß $\mathfrak{i}$ ein n-gliedriger Modulus ist. Seine Basiszahlen $\lambda_1, \lambda_2, \cdots, \lambda_n$ lassen sich durch die dortigen Formeln (53) darstellen, in denen allgemein $\mu_i' = \alpha\omega_i$ zu denken ist; da aber die Zahlen (3), weil in $\mathfrak{o}$ enthalten, ganzzahlige

lineare Funktionen der ω_i sind, gehen jene Formeln in Gleichungen von der Gestalt:

$$\lambda_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \cdots + a_{in}\omega_n \quad (i = 1, 2, \cdots, n) \tag{4}$$

über, deren Koeffizienten ganzzahlig sind und deren Determinante nach dem Schlußsatze der angeführten Nummer die Anzahl der Klassen inkongruenter Zahlen angibt, in welche die Zahlen der Ordnung $\mathfrak{o}$ (mod. $\mathfrak{i}$) verteilt werden können, in Zeichen:

$$|a_{ik}| = (\mathfrak{o}, \mathfrak{i}). \tag{5}$$

In Analogie mit der Definition der Norm für ein Körperideal nennen wir diese Anzahl die Norm des Ideals $\mathfrak{i}$ und bezeichnen sie durch $\mathfrak{N}'(\mathfrak{i})$.

Der Begriff eines Ideals in $\mathfrak{o}$ soll aber hinfort etwas enger gefaßt werden. Wir fügen ihm nämlich die neue Bestimmung hinzu, daß $\mathfrak{o}$ der größte gemeinsame Teiler von $\mathfrak{i}$ und $\mathfrak{f}$ sein solle, in Zeichen:

$$\mathfrak{i} + \mathfrak{f} = \mathfrak{o}. \tag{6}$$

Die so definierten Ringideale nennt Hilbert „regulär“. Nur scheinbar wird auf solche Weise die völlige Analogie zwischen der Definition der Ideale in $\mathfrak{o}$ und derjenigen der Körperideale gestört, in Wahrheit ist auch bei den letzteren die verlangte Eigenschaft vorhanden, denn für sie geht die Gleichung (6), da der Führer der Ordnung $\mathfrak{g}$ mit $\mathfrak{g}$ übereinstimmt (s. Kap. 4, Nr. 6) in die folgende über:

$$\mathfrak{i} + \mathfrak{g} = \mathfrak{g},$$

welche, da $\mathfrak{i} \succ \mathfrak{g}$ ist, von selber erfüllt ist. Durch Hinzufügung dieser neuen Bestimmung gewinnt man aber wesentliche Vorteile, wie z. B. darin sich kundgibt, daß die Kongruenzen

$$\omega \equiv \alpha \quad (\text{mod. } \mathfrak{i}), \quad \omega \equiv \beta \quad (\text{mod. } \mathfrak{f}),$$

in denen α, β gegebene Zahlen in $\mathfrak{o}$ sind, stets durch eine Zahl ω derselben Ordnung erfüllt werden kann (s. Kap. 2, Nr. 3).

Auf Grund dieser Bestimmung erkennt man auch, daß $\mathfrak{o}$ die „Ordnung“ eines jeden Ideales in $\mathfrak{o}$ ist. Die Ord-

nung $\mathfrak{i}^0$ eines solchen Ideals $\mathfrak{i}$ ist nämlich die Gesamtheit aller Zahlen α, für welche $\mathfrak{i}\alpha \succ \mathfrak{i}$ ist; wegen (2) gehört zu ihr jede Zahl in $\mathfrak{o}$ und folglich ist

$$(7) \qquad \mathfrak{o} \succ \mathfrak{i}^0.$$

Andererseits bestehen (Kap. 2, Nr. 2; 4, Nr. 6) die Beziehungen

$$\mathfrak{z} \succ \mathfrak{i}^0 \succ \mathfrak{g},$$

wo unter $\mathfrak{z}$ die Gesamtheit der rationalen ganzen Zahlen verstanden wird. Hieraus folgt, da für das Körperideal $\mathfrak{f}$ die Gleichungen bestehen

$$\mathfrak{z}\mathfrak{f} = \mathfrak{f}, \; \mathfrak{g}\mathfrak{f} = \mathfrak{f},$$

die Beziehung $\mathfrak{f} \succ \mathfrak{f}\mathfrak{i}^0 \succ \mathfrak{f}$, d. h.

$$\mathfrak{f}\mathfrak{i}^0 = \mathfrak{f}.$$

Da aber ferner $\mathfrak{i}\mathfrak{i}^0 = \mathfrak{i}$ ist, so ergibt die festgesetzte Gleichung (6) die folgende:

$$\mathfrak{o} = \mathfrak{i} + \mathfrak{f} = \mathfrak{o}\mathfrak{i}^0,$$

während wegen $\mathfrak{z} \succ \mathfrak{o}$ sich

$$\mathfrak{i}^0 \succ \mathfrak{z}\mathfrak{i}^0 \succ \mathfrak{o}\mathfrak{i}^0 = \mathfrak{o}$$

d. h.

$$\mathfrak{i}^0 \succ \mathfrak{o}$$

herausstellt. Diese Beziehung zusammen mit (7) gibt aber in der Tat die Gleichheit

$$(8) \qquad \mathfrak{o} = \mathfrak{i}^0.$$

Ferner gilt der Satz: Der größte gemeinsame Teiler $\mathfrak{i}' + \mathfrak{i}''$, das kleinste gemeinsame Vielfache $\mathfrak{i}' - \mathfrak{i}''$, und das Produkt $\mathfrak{i}' \cdot \mathfrak{i}''$ zweier Ideale $\mathfrak{i}'$, $\mathfrak{i}''$ in $\mathfrak{o}$ sind wieder Ideale in $\mathfrak{o}$. Es leuchtet in der Tat ohne weiteres ein, daß diese Gebilde Moduln in $\mathfrak{o}$ sind, welche die erste charakteristische Bedingung (2) erfüllen, und so bedarf es nur des Nachweises, daß ihnen auch die in (6) ausgesprochene Eigenschaft zukommt. Dies folgt

erstens für den Modulus $\mathfrak{i}' + \mathfrak{i}''$ aus den Gleichungen

$$(\mathfrak{i}' + \mathfrak{i}'') + \mathfrak{f} = \mathfrak{i}' + (\mathfrak{i}'' + \mathfrak{f}) = \mathfrak{i}' + \mathfrak{o} = \mathfrak{o},$$

deren letzte aus $\mathfrak{i}' \succ \mathfrak{o}$ hervorgeht;

zweitens ist wegen $\mathfrak{o} = \mathfrak{i}' + \mathfrak{f}$ auch $\mathfrak{o}\mathfrak{i}'' = \mathfrak{i}'\mathfrak{i}'' + \mathfrak{f}\mathfrak{i}''$; da nun

$$\mathfrak{i}'\mathfrak{i}'' \succ \mathfrak{o}\mathfrak{i}' = \mathfrak{i}', \quad \mathfrak{i}'\mathfrak{i}'' \succ \mathfrak{o}\mathfrak{i}'' = \mathfrak{i}''$$

und endlich

$$\mathfrak{i}''\mathfrak{f} \succ \mathfrak{g}\mathfrak{f} = \mathfrak{f}$$

ist, so ergibt sich zunächst $\mathfrak{i}'' \succ (\mathfrak{i}' - \mathfrak{i}'') + \mathfrak{f}$ und sodann

$$\mathfrak{o} = \mathfrak{i}'' + \mathfrak{f} \succ (\mathfrak{i}' - \mathfrak{i}'') + \mathfrak{f},$$

während selbstverständlich auch umgekehrt

$$(\mathfrak{i}' - \mathfrak{i}'') + \mathfrak{f} \succ \mathfrak{o}$$

ist, also findet sich

$$(\mathfrak{i}' - \mathfrak{i}'') + \mathfrak{f} = \mathfrak{o};$$

was drittens das Produkt $\mathfrak{i}' \cdot \mathfrak{i}''$ anbelangt, so folgt aus den vorausgesetzten Gleichungen

$$\mathfrak{o} = \mathfrak{i}' + \mathfrak{f}, \quad \mathfrak{o} = \mathfrak{i}'' + \mathfrak{f}$$

durch Multiplikation die andere:

$$\mathfrak{o} \cdot \mathfrak{o} = \mathfrak{i}' \cdot \mathfrak{i}'' + \mathfrak{i}' \cdot \mathfrak{f} + \mathfrak{i}'' \cdot \mathfrak{f} + \mathfrak{f} \cdot \mathfrak{f}$$

d. h.

$$\mathfrak{o} \succ \mathfrak{i}' \cdot \mathfrak{i}'' + \mathfrak{f},$$

während doch auch umgekehrt

$$\mathfrak{i}' \cdot \mathfrak{i}'' + \mathfrak{f} \succ \mathfrak{o}$$

ist, also ergibt sich

$$\mathfrak{i}' \cdot \mathfrak{i}'' + \mathfrak{f} = \mathfrak{o}.$$

Das Produkt $\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''$ zweier Ideale ist durch jedes derselben teilbar, d. h. in jedem von ihnen enthalten. In der Tat folgt aus $\mathfrak{i}' \succ \mathfrak{o}$ die Beziehung $\mathfrak{i} \succ \mathfrak{o}\mathfrak{i}'' = \mathfrak{i}''$, und aus $\mathfrak{i}'' \succ \mathfrak{o}$ ebenso $\mathfrak{i} \succ \mathfrak{o}\mathfrak{i}' = \mathfrak{i}'$.

2. Daß nun für die so definierten Ideale in $\mathfrak{o}$ genau dieselben Teilbarkeitsgesetze gelten, wie sie für die Körperideale im 6. Kapitel hergeleitet worden sind, erkennt man am einfachsten, indem man die Theorie der ersteren auf die der letzteren zurückführt. Dies erreicht man aber durch Beachtung einer einfachen Beziehung, die zwischen beiden besteht und sich in dem folgenden Satze aussprechen läßt:

Jedem Ideale der Ordnung $\mathfrak{o}$ entspricht ein bestimmtes zum Führer $\mathfrak{f}$ der Ordnung relativ primes Körperideal, und umgekehrt.

In der Tat, wenn $\mathfrak{i}$ ein Ideal in $\mathfrak{o}$ ist, so ist $\mathfrak{g}\mathfrak{i}$ jedenfalls ein Körperideal, da dies Produkt ein in $\mathfrak{g}$ enthaltener Modulus und $\mathfrak{g}\cdot\mathfrak{g}\mathfrak{i} = \mathfrak{g}\mathfrak{i}$ ist; aus $\mathfrak{i} + \mathfrak{f} = \mathfrak{o}$ folgt aber zudem $\mathfrak{g}\mathfrak{i} + \mathfrak{g}\mathfrak{f} = \mathfrak{g}\mathfrak{o}$, d. i. $\mathfrak{g}\mathfrak{i} + \mathfrak{f} = \mathfrak{g}$, womit der erste Teil der Behauptung erwiesen ist. Denkt man sich $\mathfrak{i}$ als Modulus:

$$\mathfrak{i} = [\lambda_1, \lambda_2, \cdots, \lambda_n],$$

so erkennt man, daß $\mathfrak{g}\mathfrak{i} \succ \mathfrak{g}\lambda_1 + \mathfrak{g}\lambda_2 + \cdots + \mathfrak{g}\lambda_n$ ist; da aber auch jedes der Produkte $\mathfrak{g}\lambda_k$ in $\mathfrak{g}\mathfrak{i}$ enthalten ist, muß auch $\mathfrak{g}\lambda_1 + \mathfrak{g}\lambda_2 + \cdots + \mathfrak{g}\lambda_n \succ \mathfrak{g}\mathfrak{i}$ sein, und somit erweist sich das Körperideal $\mathfrak{g}\mathfrak{i}$, welches dem Ideale $\mathfrak{i}$ in $\mathfrak{o}$ entspricht, als der größte gemeinsame Idealteiler von den Basiszahlen oder Elementen von $\mathfrak{i}$. — Ferner ist $\mathfrak{i}$ das kleinste gemeinsame Vielfache von $\mathfrak{g}\mathfrak{i}$ und $\mathfrak{o}$, in Zeichen:

$$\mathfrak{i} = \mathfrak{g}\mathfrak{i} - \mathfrak{o}. \tag{9}$$

Denn jede Zahl α, welche in $\mathfrak{g}\mathfrak{i}$ und $\mathfrak{o}$ enthalten ist, kann wegen $\mathfrak{i} + \mathfrak{f} = \mathfrak{o}$ gleich $\beta + \varphi$ gesetzt werden, wo β eine Zahl in $\mathfrak{i}$ und φ eine Zahl in $\mathfrak{f}$ bedeutet; da aber $\varphi = \alpha - \beta$ auch in $\mathfrak{g}\mathfrak{i}$ mithin in $\mathfrak{g}\mathfrak{i} - \mathfrak{f}$ enthalten ist, so ergibt sich die Beziehung

$$\mathfrak{g}\mathfrak{i} - \mathfrak{o} \succ \mathfrak{i} + (\mathfrak{g}\mathfrak{i} - \mathfrak{f});$$

umgekehrt ist jede Zahl $\beta + \varphi$, wo β eine in $\mathfrak{i}$ und φ eine zugleich in $\mathfrak{g}\mathfrak{i}$ und $\mathfrak{f}$ enthaltene Zahl ist, sowohl eine Zahl in $\mathfrak{g}\mathfrak{i}$ als eine solche in $\mathfrak{o}$, also findet sich auch umgekehrt

$$\mathfrak{i} + (\mathfrak{g}\mathfrak{i} - \mathfrak{f}) \succ \mathfrak{g}\mathfrak{i} - \mathfrak{o},$$

daher endlich

$$\mathfrak{g}\mathfrak{i} - \mathfrak{o} = \mathfrak{i} + (\mathfrak{g}\mathfrak{i} - \mathfrak{f}). \tag{10}$$

Nach der Idealtheorie (6. Kap., Formel (95)) ist aber

$$(\mathfrak{g}\mathfrak{i} + \mathfrak{f}) \cdot (\mathfrak{g}\mathfrak{i} - \mathfrak{f}) = \mathfrak{g}\mathfrak{i} \cdot \mathfrak{f}$$

oder

$$\mathfrak{g}\mathfrak{i} - \mathfrak{f} = \mathfrak{i} \cdot \mathfrak{f},$$

die Formel (10) verwandelt sich also in

$$\mathfrak{g}\mathfrak{i} - \mathfrak{o} = \mathfrak{i} + \mathfrak{i} \cdot \mathfrak{f} = (\mathfrak{o} + \mathfrak{f})\,\mathfrak{i} = \mathfrak{o}\mathfrak{i} = \mathfrak{i},$$

w. z. b. w.

Da weiter

$$\mathfrak{g} = \mathfrak{g}\mathfrak{i} + \mathfrak{f} \succ \mathfrak{g}\mathfrak{i} + \mathfrak{o} \succ \mathfrak{g}$$

also

$$\mathfrak{g}\mathfrak{i} + \mathfrak{o} = \mathfrak{g} \tag{11}$$

ist, so ist $\mathfrak{g}$ der größte gemeinsame Teiler von $\mathfrak{g}\mathfrak{i}$ und $\mathfrak{o}$.

Um nun den zweiten Teil der Behauptung zu erweisen, sei $\mathfrak{j}$ ein beliebiges zu $\mathfrak{f}$ relativ primes Körperideal, also

$$\mathfrak{j} + \mathfrak{f} = \mathfrak{g}, \tag{12}$$

und $\mathfrak{i}$ bezeichne das kleinste gemeinsame Vielfache von $\mathfrak{j}$ und $\mathfrak{o}$, in Zeichen:

$$\mathfrak{i} = \mathfrak{j} - \mathfrak{o}. \tag{13}$$

Dieser in $\mathfrak{o}$ enthaltene Zahlenmodulus $\mathfrak{i}$ erfüllt aber die Bedingung (2), denn, gehört die Zahl α sowohl zum Ideale $\mathfrak{j}$ als zur Ordnung $\mathfrak{o}$, und ist ω irgend eine Zahl der letzteren, so gehört auch $\omega\alpha$ sowohl zu $\mathfrak{j}$ als auch zu $\mathfrak{o}$ und demnach zu $\mathfrak{i}$. Nun kann wegen (12) jede Zahl in $\mathfrak{g}$ also auch jede in $\mathfrak{o}$ enthaltene Zahl ω gleich $\alpha + \varphi$ gesetzt werden, wo φ zu $\mathfrak{f}$ und α zu $\mathfrak{j}$ gehört; da hieraus aber $\alpha = \omega - \varphi$ sich auch als eine zu $\mathfrak{o}$ gehörige Zahl ergibt, so ist

$$\omega = \alpha + \varphi,$$

wo α zu $\mathfrak{j} - \mathfrak{o}$ und φ zu $\mathfrak{f}$ gehört, mithin findet sich

$$\mathfrak{o} \succ (\mathfrak{j} - \mathfrak{o}) + \mathfrak{f},$$

während offenbar auch umgekehrt

$$(\mathfrak{j} - \mathfrak{o}) + \mathfrak{f} \succ \mathfrak{o}$$

ist, und daher folgt

$$\mathfrak{i} + \mathfrak{f} = (\mathfrak{j} - \mathfrak{o}) + \mathfrak{f} = \mathfrak{o},$$

der Modulus $\mathfrak{i}$ erfüllt demnach auch die zweite charakteristische Bedingung (6) und kennzeichnet sich dadurch als ein Ideal in $\mathfrak{o}$.

Hiernach ist $\mathfrak{g}\mathfrak{i}$ ein zu $\mathfrak{f}$ relativ primes Körperideal, von welchem leicht zu erkennen ist, daß es identisch ist mit $\mathfrak{j}$. In der Tat folgt aus $\mathfrak{i} \succ \mathfrak{j}$ zunächst $\mathfrak{g}\mathfrak{i} \succ \mathfrak{g}\mathfrak{j} = \mathfrak{j}$. Andererseits aber führt die Gleichung $\mathfrak{g}\mathfrak{i} + \mathfrak{f} = \mathfrak{g}$ zu der andern:

$$\mathfrak{g}\mathfrak{i} \cdot \mathfrak{j} + \mathfrak{f}\mathfrak{j} = \mathfrak{j},$$

aus welcher, da zugleich

$$\mathfrak{f}\mathfrak{j} \succ \mathfrak{j} \quad \text{und} \quad \mathfrak{f}\mathfrak{j} \succ \mathfrak{f} \succ \mathfrak{o}$$

und somit $\mathfrak{f}\mathfrak{j} \succ \mathfrak{i} = \mathfrak{j} - \mathfrak{o} \succ \mathfrak{g}\mathfrak{i}$ ist, das Körperideal $\mathfrak{j}$ als teilbar durch $\mathfrak{g}\mathfrak{i}$, d. i. umgekehrt $\mathfrak{j} \succ \mathfrak{g}\mathfrak{i}$, im ganzen also $\mathfrak{j} = \mathfrak{g}\mathfrak{i}$ hervorgeht.

Durch diesen Doppelsatz ist eine feste Korrespondenz hergestellt zwischen den Idealen $\mathfrak{i}$ in $\mathfrak{o}$ auf der einen, und den zu $\mathfrak{f}$ relativ primen Körperidealen $\mathfrak{j}$ auf der anderen Seite, welche darin ihren Ausdruck findet, daß gleichzeitig

$$\mathfrak{j} = \mathfrak{g}\mathfrak{i} \quad \text{und} \quad \mathfrak{i} = \mathfrak{j} - \mathfrak{o}$$

ist. Insbesondere sind auf solche Weise offenbar die Ideale $\mathfrak{g}$ und $\mathfrak{o}$ mit einander verbunden.

Da successive (vgl. (11))

$$\mathfrak{g}\mathfrak{i} + \mathfrak{o} = \mathfrak{g}\mathfrak{i} + \mathfrak{i} + \mathfrak{f} = (\mathfrak{g} + \mathfrak{o})\mathfrak{i} + \mathfrak{f} = \mathfrak{g}\mathfrak{i} + \mathfrak{f} = \mathfrak{g}$$

gefunden wird, so ergibt sich einerseits

$$(\mathfrak{o},\ \mathfrak{g}\mathfrak{i}) = (\mathfrak{o},\ \mathfrak{g}\mathfrak{i} - \mathfrak{o}) = (\mathfrak{o},\ \mathfrak{i})$$

andererseits

$$(\mathfrak{o},\ \mathfrak{g}\mathfrak{i}) = (\mathfrak{o} + \mathfrak{g}\mathfrak{i},\ \mathfrak{g}\mathfrak{i}) = (\mathfrak{g},\ \mathfrak{g}\mathfrak{i})$$

und folglich

$$(\mathfrak{o},\ \mathfrak{i}) = (\mathfrak{g},\ \mathfrak{g}\mathfrak{i})$$

d. h.

$$\mathfrak{N}'(\mathfrak{i}) = \mathfrak{N}(\mathfrak{g}\mathfrak{i}) = \mathfrak{N}(\mathfrak{j}) \tag{14}$$

als die zwischen den Normen der einander entsprechenden Ideale $\mathfrak{i}$, $\mathfrak{j}$ bestehende Beziehung.

Endlich leuchtet ein, daß, wenn $\mathfrak{i}'$, $\mathfrak{i}''$ zwei Ideale in $\mathfrak{o}$ sind, für welche

$$\mathfrak{g}\mathfrak{i}' = \mathfrak{g}\mathfrak{i}'' \tag{15}$$

ist, stets auch

$$\mathfrak{i}' = \mathfrak{i}''$$

sein muß. Denn den vorigen Entwicklungen zufolge ist

$$\mathfrak{i}' = \mathfrak{o} - \mathfrak{g}\mathfrak{i}', \quad \mathfrak{i}'' = \mathfrak{o} - \mathfrak{g}\mathfrak{i}'',$$

woraus die Behauptung unmittelbar sich bestätigt.

Aus diesen Ergebnissen folgt nun sehr leicht ein neuer

Satz, welcher die Grundlage für die Arithmetik der Ideale in $\mathfrak{o}$ bildet. Das Produkt $\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''$ zweier Ideale $\mathfrak{i}'$, $\mathfrak{i}''$ in $\mathfrak{o}$ ist, wie gezeigt worden, wieder ein Ideal in $\mathfrak{o}$, das in jedem der ersteren enthalten oder, wie anders gesagt werden darf, durch sie teilbar ist, mit anderen Worten: jeder Faktor eines Ideals ist auch ein Teiler desselben. Es wird auch hier wesentlich nun darauf ankommen, die Umkehrung zu beweisen, daß nämlich jeder Teiler eines Ideals $\mathfrak{i}$ in $\mathfrak{o}$ ein Faktor desselben ist, oder daß, wenn $\mathfrak{i}$ teilbar ist durch ein Ideal $\mathfrak{i}'$ in $\mathfrak{o}$, ein zweites Ideal $\mathfrak{i}''$ in $\mathfrak{o}$ vorhanden ist von der Beschaffenheit, daß $\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''$ gesetzt werden kann. Dies erkennt man aber einfach folgendermaßen. Ist $\mathfrak{i}$ teilbar durch $\mathfrak{i}'$, in Zeichen: $\mathfrak{i} \succ \mathfrak{i}'$, so ist auch $\mathfrak{g}\mathfrak{i} \succ \mathfrak{g}\mathfrak{i}'$ und somit der früheren Idealtheorie zufolge ein Ideal $\mathfrak{j}''$ des Körpers vorhanden, für welches

$$\mathfrak{g}\mathfrak{i} = \mathfrak{g}\mathfrak{i}' \cdot \mathfrak{j}''$$

ist. Da aber das Ideal $\mathfrak{g}\mathfrak{i}$ zu $\mathfrak{f}$ relativ prim ist, muß dasselbe auch gelten für das Körperideal $\mathfrak{j}''$ und demnach ein Ideal $\mathfrak{i}''$ — und dem letzten Satze zufolge nur ein einziges — in $\mathfrak{o}$ vorhanden sein, für welches $\mathfrak{g}\mathfrak{i}'' = \mathfrak{j}''$ ist, sodaß die vorige Gleichung die Gestalt annimmt:

$$\mathfrak{g}\mathfrak{i} = \mathfrak{g}\mathfrak{i}' \cdot \mathfrak{g}\mathfrak{i}'' = \mathfrak{g} \cdot \mathfrak{i}'\mathfrak{i}'',$$

worin auch $\mathfrak{i}'\mathfrak{i}''$ ein Ideal in $\mathfrak{o}$ ist, und wodurch dann nach dem letzten Satze sich

$$\mathfrak{i} = \mathfrak{i}'\mathfrak{i}''$$

ergibt. Es gibt aber auch nur ein einziges Ideal $\mathfrak{i}''$ in $\mathfrak{o}$ von dieser Art; denn, wäre $\mathfrak{i}'''$ noch ein zweites, sodaß auch

$$\mathfrak{i} = \mathfrak{i}'\mathfrak{i}'''$$

gesetzt werden kann, so würde daraus

$$\mathfrak{i}'\mathfrak{i}'' = \mathfrak{i}'\mathfrak{i}'''$$

und weiter die Gleichung

$$\mathfrak{g}\mathfrak{i}' \cdot \mathfrak{g}\mathfrak{i}'' = \mathfrak{g}\mathfrak{i}' \cdot \mathfrak{g}\mathfrak{i}''',$$

folglich der früheren Idealtheorie zufolge $\mathfrak{g}\mathfrak{i}'' = \mathfrak{g}\mathfrak{i}'''$ und nun wieder nach dem letzten Satze $\mathfrak{i}'' = \mathfrak{i}'''$ folgen.

Diese Resultate lassen deutlich erkennen, daß für die Ideale einer beliebigen Ordnung ganz dieselben Teilbarkeitsgesetze Bestand haben müssen, wie sie für die Körperideale im 6. Kapitel gegeben worden sind. Es ist daher nicht nötig, hierauf noch weiter einzugehen; nur die Formel

$$\mathfrak{N}'(\mathfrak{i}'\mathfrak{i}'') = \mathfrak{N}'(\mathfrak{i}') \cdot \mathfrak{N}'(\mathfrak{i}'') \tag{16}$$

zur Bildung der Norm eines Produkts von Idealen in $\mathfrak{o}$ aus den Normen seiner Faktoren sei noch bemerkt. Sie ergibt sich sogleich, wenn man bedenkt, daß nach (14)

$$\begin{aligned} \mathfrak{N}'(\mathfrak{i}') &= \mathfrak{N}(\mathfrak{g}\mathfrak{i}') \\ \mathfrak{N}'(\mathfrak{i}'') &= \mathfrak{N}(\mathfrak{g}\mathfrak{i}'') \\ \mathfrak{N}'(\mathfrak{i}'\mathfrak{i}'') &= \mathfrak{N}(\mathfrak{g}\mathfrak{i}'\mathfrak{i}'') \end{aligned}$$

gesetzt werden kann, die letztgeschriebene Norm aber nach Kap. 6, Formel (110)

$$\mathfrak{N}(\mathfrak{g}\mathfrak{i}'\mathfrak{i}'') = \mathfrak{N}(\mathfrak{g}\mathfrak{i}' \cdot \mathfrak{g}\mathfrak{i}'') = \mathfrak{N}(\mathfrak{g}\mathfrak{i}') \cdot \mathfrak{N}(\mathfrak{g}\mathfrak{i}'')$$

gefunden wird.

3. Nun läßt sich auch der Begriff der Äquivalenz von Idealen auf die Ideale in $\mathfrak{o}$ übertragen und dann die Verteilung der letzteren in Klassen äquivalenter Ideale bewirken. Jedoch kehren wir einstweilen hier wieder zur Ordnung $\mathfrak{g}$ sämtlicher ganzen Zahlen des Körpers zurück. Zwei Körperideale $\mathfrak{j}$, $\mathfrak{j}'$ wurden äquivalent genannt, wenn es ganze Zahlen α, α' des Körpers gibt von der Beschaffenheit, daß

$$\alpha'\mathfrak{j} = \alpha\mathfrak{j}' \tag{17}$$

ist, oder, indem der Quotient ganzer Zahlen des Körpers eine gebrochene Zahl genannt wird, wenn eine gebrochene Zahl β vorhanden ist, für welche

$$\mathfrak{j}' = \beta\mathfrak{j} \tag{18}$$

ist. Es sei bemerkt, daß diese Beziehung zweier Ideale zu einander auch auf eine andere Weise ausgedrückt werden kann. Nach dem Fundamentalsatze des 6. Kapitels gibt es für jedes Ideal $\mathfrak{j}$ ein zugehöriges anderes Ideal $\mathfrak{m}$ von der Art, daß $\mathfrak{j}\mathfrak{m}$ ein Hauptideal $\mathfrak{g}\alpha$ wird. Besteht nun die Beziehung (18), so folgt

$$\mathfrak{j}'\mathfrak{m} = \beta \cdot \mathfrak{j}\mathfrak{m} = \mathfrak{g} \cdot \alpha\beta,$$

nach welcher Gleichung die im Modulus der rechten Seite

enthaltene Zahl $\alpha\beta$, weil auch in dem Ideale der linken Seite enthalten, gewiß eine ganze Zahl, $\mathfrak{g} \cdot \alpha\beta$ also ein Hauptideal sein wird; demnach ist mit $\mathfrak{j} \cdot \mathfrak{m}$ zugleich auch $\mathfrak{j}' \cdot \mathfrak{m}$ ein Hauptideal. Umgekehrt aber, wenn zugleich

$$\mathfrak{j}\mathfrak{m} = \mathfrak{g}\alpha, \quad \mathfrak{j}'\mathfrak{m} = \mathfrak{g}\alpha' \tag{19}$$

Hauptideale sind, so folgt

$$\alpha'\mathfrak{j}\mathfrak{m} = \alpha\mathfrak{j}'\mathfrak{m}$$

und hieraus die Gleichung (17), d. i. die Äquivalenz von $\mathfrak{j}$ und $\mathfrak{j}'$. Die Äquivalenz zweier Körperideale kann demnach, wenn man will, auch dahin formuliert werden, daß zwei Ideale $\mathfrak{j}$, $\mathfrak{j}'$ äquivalent genannt werden, wenn sie durch ein- und dasselbe Ideal $\mathfrak{m}$ multipliziert zu Hauptidealen werden. Geschieht übrigens dies durch ein Ideal $\mathfrak{m}$, so geschieht es durch jedes Ideal $\mathfrak{n}$, welches eins der beiden Ideale zu einem Hauptideale macht, denn, ist $\mathfrak{j} \cdot \mathfrak{n} = \mathfrak{g}\gamma$, so folgt aus (18)

$$\mathfrak{j}' \cdot \mathfrak{n} = \mathfrak{g} \cdot \beta\gamma,$$

in welcher Gleichung sich wieder $\beta\gamma$ als ganze Zahl, $\mathfrak{g} \cdot \beta\gamma$ also als Hauptideal ergibt. Daher sind dann wieder zwei Ideale, welche demselben dritten Ideale äquivalent sind, es auch unter einander, und hierdurch ermöglicht sich die Verteilung aller Ideale in Klassen äquivalenter Ideale.

Aber es soll fortan der Begriff der Äquivalenz etwas enger gefaßt werden.

Zwei Ideale $\mathfrak{j}$, $\mathfrak{j}'$ sollen nämlich nur dann äquivalent heißen, wenn die Zahl β in der Beziehung (18) eine positive Norm, oder, was dasselbe sagt, wenn die Zahlen α, α' in den Beziehungen (17) oder (19) Normen von demselben Vorzeichen besitzen; andernfalls nennen wir die durch die gedachten Beziehungen verbundenen Ideale halbäquivalent. Gibt es im Körper keine Zahlen β von negativer Norm, so werden auch jetzt noch alle Ideale von der Form (18) die Klasse der mit $\mathfrak{j}$ äquivalenten Ideale ausmachen; andernfalls zerfällt die bisherige Klasse der mit $\mathfrak{j}$ äquivalenten Ideale nach der neuen Definition in zwei voneinander zu scheidende Klassen, indem die sämtlichen Ideale von der Form (18), in welcher β nur Zahlen des Körpers mit positiver Norm durch-

läuft, die jetzige engere Klasse der mit $\mathfrak{j}$ äquivalenten Ideale ausmachen, während die Ideale derselben Form, in der β nur Zahlen des Körpers mit negativer Norm durchläuft, ebenfalls eine besondere Klasse äquivalenter Ideale zusammensetzen, indem in der Tat zwischen je zweien derselben:

$$\mathfrak{j}' = \beta'\mathfrak{j}, \quad \mathfrak{j}'' = \beta''\mathfrak{j}$$

eine Beziehung $\mathfrak{j}'' = \frac{\beta''}{\beta'} \cdot \mathfrak{j}'$ besteht, in welcher $\frac{\beta''}{\beta'}$ eine positive Norm hat. — Gibt es keine Einheiten mit negativer Norm, so werden beide Klassen voneinander verschieden sein; denn, gehören $\beta\mathfrak{j}$ und $\beta'\mathfrak{j}$, wo $N(\beta) > 0$, $N(\beta') < 0$ gedacht wird, diesen beiden Klassen an, so könnte die Gleichheit $\beta\mathfrak{j} = \beta'\mathfrak{j}$ nur bestehen, wenn $\beta' = \beta\varepsilon$ und ε eine Einheit wäre, deren Norm dann negativ ist. In diesem Falle zerlegt sich also jede der früheren Klassen in zwei, und die Anzahl aller Klassen äquivalenter Ideale verdoppelt sich. Ist dagegen eine Einheit ε mit negativer Norm vorhanden, so fallen die beiden Klassen zusammen, da wegen $\varepsilon \cdot \mathfrak{j} = \mathfrak{j}$ zugleich mit der Gleichung $\mathfrak{j}' = \beta\mathfrak{j}$ auch die Gleichung $\mathfrak{j}' = \beta\varepsilon \cdot \mathfrak{j}$ besteht; in diesem Falle bleibt mithin wieder trotz der engeren Äquivalenz die Verteilung der Ideale in Klassen und deren Anzahl unverändert dieselbe. Im ersteren Falle besteht bei der neuen Fassung des Äquivalenzbegriffes die Hauptklasse H ersichtlich nur aus all' denjenigen Hauptidealen $\mathfrak{g}\gamma$, welche den ganzen Zahlen γ mit positiver Norm entsprechen; aber auch im andern Falle dürfen und wollen wir fortan unter einem *Hauptideale* $\mathfrak{g}\gamma$ stets ein solches verstehen, welches einer Zahl γ *mit positiver Norm* entspricht.

Sind nun $\mathfrak{j}$, $\mathfrak{j}_1$ die Repräsentanten zweier Klassen C, C_1 der neuen Einteilung, und

$$\mathfrak{j}' = \beta\mathfrak{j}, \quad \mathfrak{j}_1' = \beta_1\mathfrak{j}_1$$

die übrigen in diesen Klassen resp. enthaltenen Ideale, sodaß β, β_1 nur Zahlen mit positiver Norm durchlaufen, so erhält man durch die Formel

$$\mathfrak{j}' \cdot \mathfrak{j}_1' = \beta\beta_1 \cdot \mathfrak{j}\mathfrak{j}_1$$

unendlich viel Ideale, welche sämtlich ein- und derselben

Klasse C_2 angehören, denn jedes der Produkte $\beta\beta_1$ hat auch eine positive Norm; man darf daher

$$C_2 = C \cdot C_1$$

setzen und diese Klasse C_2, welche durch das in ihr befindliche Ideal $\mathfrak{j}\mathfrak{j}_1$ repräsentiert werden kann, die aus C und C_1 zusammengesetzte Klasse nennen. Hiernach leuchtet ein, daß die Gesetze der Zusammensetzung der Klassen durch die engere Definition der Äquivalenz in keiner Weise geändert werden können.

Insbesondere mag folgender Satz festgestellt werden: In jeder der neuen Klassen C gibt es ein Ideal $\mathfrak{j}$, das zu einem beliebig gegebenen Ideale relativ prim ist. Sei nämlich C' die zu C entgegengesetzte Klasse, diejenige nämlich, für welche

$$C \cdot C' = H$$

ist, und $\mathfrak{a}$ irgend ein Ideal dieser Klasse, $\mathfrak{b}$ aber das gegebene Ideal, so gibt es nach Kap. 6, Nr. 16 eine ganze Zahl ω der Art, daß

$$\mathfrak{a}\mathfrak{b} + \mathfrak{g}\omega = \mathfrak{a} \tag{20}$$

ist; bezeichnet aber γ irgend eine mit ω (mod. $\mathfrak{a}\mathfrak{b}$) kongruente Zahl, sodaß $\omega = \gamma + \alpha$ gesetzt werden kann, unter α eine Zahl in $\mathfrak{a}\mathfrak{b}$ verstanden, so findet sich, da $\mathfrak{a}\mathfrak{b} + \mathfrak{g}\alpha = \mathfrak{a}\mathfrak{b}$ ist, aus (20) auch die Gleichung

$$\mathfrak{a}\mathfrak{b} + \mathfrak{g}\gamma = \mathfrak{a}, \tag{21}$$

derzufolge $\mathfrak{g}\gamma \succ \mathfrak{a}$ ist; man darf daher setzen

$$\mathfrak{g}\gamma = \mathfrak{a} \cdot \mathfrak{j}, \tag{22}$$

wo $\mathfrak{j}$ ein Ideal bezeichnet, das offenbar der zu $\mathfrak{a}$ entgegengesetzten Klasse, d. h. der Klasse C angehören muß, wenn die ganze Zahl γ so gewählt worden ist, daß ihre Norm positiv ist. Daß solche Wahl aber möglich ist, erkennt man aus dem folgenden allgemeinen Satze:

Ist $\mathfrak{m}$ ein n-gliedriger Modulus des Körpers und ω eine gegebene ganze Zahl des letzteren, so gibt es unter den mit ω (mod. $\mathfrak{m}$) kongruenten Zahlen immer solche, deren Norm positiv ist. Dies versteht sich von selbst, wenn der Körper mit allen seinen Konjugierten imaginär

ist, da alsdann die unter einander konjugierten Zahlen stets zu zweien konjugiert imaginär sind, ihr Produkt, d. i. die Norm einer beliebigen Zahl des Körpers also positiv ist. Entgegengesetzten Falls bemerke man, daß, weil die Basis des Modulus zugleich eine solche des Körpers ist, jede Zahl des letzteren, insbesondere also auch die darin befindliche Eins mit einer rationalen ganzen Zahl m multipliziert eine Zahl des Modulus werden muß; mit anderen Worten: es gibt eine rationale ganze Zahl m von der Art, daß $m \equiv 0 \pmod{\mathfrak{m}}$ und daher für jeden rational ganzzahligen Wert h auch $m \cdot h \equiv 0 \pmod{\mathfrak{m}}$ ist. Daher ist dann

$$\gamma = \omega + h \cdot m \equiv \omega \pmod{\mathfrak{m}}.$$

Bildet man nun die Norm $N(\gamma)$, d. h. das Produkt

$$(\omega^{(1)} + hm)(\omega^{(2)} + hm) \cdots (\omega^{(n)} + hm),$$

so läßt sich h so groß wählen, daß die sämtlichen reellen Faktoren desselben positiv werden, während die übrigen als paarweise konjugiert imaginär positive Produkte ergeben, also wird dann $N(\gamma) > 0$, wie behauptet.

Diesem Satze zufolge gehört also das durch die Beziehung (22) bestimmte Ideal $\mathfrak{j}$ bei passender Wahl der Zahl γ der Klasse C an. Da nun vermöge derselben Beziehung aus (21)

$$\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{j} = \mathfrak{a}$$

d. i.

$$\mathfrak{b} + \mathfrak{j} = \mathfrak{g}$$

hervorgeht, so ist dasselbe Ideal $\mathfrak{j}$ relativ prim zu dem gegebenen Ideale $\mathfrak{b}$, wie es verlangt wurde.

4. Schon in Kap. 6, Nr. 8 ist gezeigt worden, daß die Anzahl der Klassen äquivalenter Ideale endlich ist. Bei der Wichtigkeit dieses Umstandes wird es erwünscht sein, noch einen zweiten, auf ganz anderer Grundlage ruhenden Beweis dafür kennen zu lernen, wie er nun zunächst hier gegeben werden soll. Jene Grundlage ist der

Hilfssatz: In jedem Modulus $\mathfrak{a}$ in $\mathfrak{g}$ gibt es eine von Null verschiedene Zahl α, deren Norm die Bedingung erfüllt

$$N(\alpha) \text{ absolut } \overline{\leq} \mathfrak{N}(\mathfrak{a}) \cdot A, \tag{23}$$

wo A eine nur von dem Körper abhängige endliche

Konstante bedeutet. Man kann dies folgendermaßen einsehen. Ist wieder

$$(24)\qquad w_0 = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_n u_n$$

die Fundamentalform des Körpers und legt man den Unbestimmten u_i ganzzahlige Werte aus der Reihe $0, 1, 2, \cdots, k$ bei, so entstehen $(k+1)^n$ verschiedene Zahlen in $\mathfrak{g}$. Nun bedeutet $\mathfrak{N}(\mathfrak{a}) = (\mathfrak{g}, \mathfrak{a})$ die Anzahl der (mod. $\mathfrak{a}$) inkongruenten Zahlen in $\mathfrak{g}$. Wählt man daher k so, daß

$$k^n \gtreqless \mathfrak{N}(\mathfrak{a}) < (k+1)^n$$

wird, so müssen wenigstens zwei verschiedene der aus (24) erhaltenen $(k+1)^n$ Zahlen — wir nennen sie γ', γ'' — einander (mod. $\mathfrak{a}$) kongruent, also ihre Differenz

$$\alpha = \gamma' - \gamma''$$

eine von Null verschiedene Zahl des Modulus $\mathfrak{a}$ sein. Da aber ihre Koeffizienten u_i absolut nicht größer sind als k, so muß notwendig

$$(25)\qquad \alpha \text{ absolut } \gtreqless [\text{abs. } \gamma_1 + \cdots + \text{abs. } \gamma_n] \cdot k$$

sein und eine ähnliche Ungleichheit für die mit α konjugierten Werte bestehen. Daraus folgt dann für die Norm $N(\alpha)$ eine Ungleichheit von der Form:

$$N(\alpha) \text{ abs. } \gtreqless k^n \cdot A \gtreqless \mathfrak{N}(\mathfrak{a}) \cdot A,$$

wenn unter A das Produkt der Multiplikatoren von k in der Formel (25) und den für die Konjugierten geltenden verstanden wird, eine endliche Größe, die in der Tat nur von der Basis von $\mathfrak{g}$, d. h. vom Körper selbst abhängt.

Dasselbe läßt sich auch auf Grund des Minkowskischen Satzes aus den Betrachtungen in Nr. 7 vorigen Kapitels feststellen. Bezeichnen nämlich die dortigen Zeichen $\omega_1, \omega_2, \cdots, \omega_n$ jetzt eine Basis des Modulus $\mathfrak{a}$, welche mit den Basiszahlen γ_i von $\mathfrak{g}$ durch n ganzzahlige Gleichungen

$$\omega_i = c_{i1}\gamma_1 + c_{i2}\gamma_2 + \cdots + c_{in}\gamma_n$$
$$(i = 1, 2, \cdots, n)$$

verbunden sind, deren Determinante $|c_{ik}|$ von Null verschieden ist, so wird das Zeichen Δ an der angeführten Stelle den Absolutwert der Quadratwurzel aus der Diskriminante

$$\Delta(\omega_1, \omega_2, \cdots, \omega_n) = |c_{ik}|^2 \cdot \mathrm{D},$$

wo D die Grundzahl des Körpers ist, bedeuten. Nach dem dort ausgeführten Betrachtungen ist es möglich, die Unbestimmten u_i in der Form

$$\omega_1 u_1 + \omega_2 u_2 + \cdots + \omega_n u_n$$

als ganze Zahlen, d. i. eine Zahl α des Modulus $\mathfrak{a}$ so zu wählen, daß die dort mit $\mathfrak{f}_i$ bezeichneten Formen den Ungleichheiten

$$\mathfrak{f}_i \lesseqgtr C_i \cdot \sqrt[n]{\Delta}$$

genügen, aus denen dann

$$N(\alpha) \text{ abs.} \lesseqgtr \Delta \lesseqgtr |c_{ik}| \sqrt{\mathrm{D}}$$

hervorgeht. Dem Schlußsatze des zweiten Kapitels zufolge bedeutet aber die Determinante $|c_{ik}|$ die Anzahl $(\mathfrak{g}, \mathfrak{a}) = \mathfrak{N}(\mathfrak{a})$, und somit ist nicht nur die Formel (23) bestätigt, sondern auch die nicht unwichtige fernere Erkenntnis gewonnen, daß unter der Konstanten A die Quadratwurzel aus der Grundzahl des Körpers verstanden werden darf.[1])

Um nun die Endlichkeit der Anzahl nicht äquivalenter Idealklassen zu erweisen, folgern wir aus dem Hilfssatze den anderen Satz: In jeder Idealklasse C gibt es ein Ideal $\mathfrak{j}$, dessen Norm die Konstante A nicht überschreitet. In der Tat, versteht man unter dem Modulus $\mathfrak{a}$ des Hilfssatzes irgend eins der Ideale, welche der zu C entgegengesetzten Klasse C' angehören, so folgt, da mit α auch das Ideal $\mathfrak{g}\alpha$ in $\mathfrak{a}$ enthalten ist, eine Gleichung

$$\mathfrak{g}\alpha = \mathfrak{a} \cdot \mathfrak{j},$$

unter $\mathfrak{j}$ ein Ideal verstanden, welches notwendig der zu C' entgegengesetzten Klasse C angehört.[2]) Da nun aus der vorstehenden Gleichung

$$N(\alpha) \text{ abs.} = \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{j})$$

1) Siehe über eine noch geringere Grenze Minkowski, Journ. f. Math. 107, p. 278 und Par. Comptes R. 92, p. 209.

2) In diesem Augenblicke fassen wir zwar die Äquivalenz und die Klasse in dem weiteren Sinne, wie früher; aus der Endlichkeit der Klassenanzahl in diesem Sinne folgt jedoch auch diejenige der Klassenanzahl im engeren Sinne, da diese, wie bemerkt worden, höchstens das Doppelte der ersteren ist.

folgt, so ergibt sich durch Verbindung mit (23) die behauptete Ungleichheit

$$\mathfrak{N}(\mathfrak{j}) \lesseqgtr A. \tag{26}$$

Bedenkt man jetzt, daß es unterhalb A nur eine endliche Anzahl rationaler ganzer Zahlen gibt, deren einer $\mathfrak{N}(\mathfrak{j})$ gleich sein muß, daß ferner das Ideal $\mathfrak{j}$ stets ein Teiler seiner Norm ist, und daß endlich jede rationale ganze Zahl oder, was dasselbe sagt, das ihr entsprechende Hauptideal nur eine endliche Anzahl Idealteiler besitzt, so folgt notwendig, daß die Anzahl der Ideale $\mathfrak{j}$, welche der Ungleichheit (26) genügen, und, da sie sich auf die Idealklassen in solcher Weise verteilen müssen, daß jede mindestens eins von ihnen enthält, auch die Anzahl der Idealklassen nur eine endliche sein kann.

5. Bevor wir dazu übergehen, diese Anzahl, welche h heiße, zu bestimmen, wollen wir zeigen, wie sämtliche Idealklassen durch eine Anzahl von ihnen, die man deshalb Fundamentalklassen nennen darf, ausgedrückt werden können. Die Idealklassen bilden offenbar eine endliche Gruppe von der Ordnung h, da die Multiplikation zweier von ihnen stets wieder eine Idealklasse ergibt. Diese Multiplikation ist zudem, wie diejenige der Ideale selbst, sowohl kommutativ als auch assoziativ, und deshalb gilt für die Gruppe der Idealklassen ein allgemeiner von Kronecker bewiesener Gruppensatz, der in des Verfassers „Elemente der Zahlentheorie" p. 79—88 entwickelt worden ist. Indessen mag der Beweis desselben an dieser Stelle im Anschluß an Hilberts Darstellung (Bericht über die Theorie der Zahlkörper, p. 233) kurz reproduziert werden.

Da nach Kap. 6, Nr. 9 die h^{te} Potenz jeder Klasse C der Hauptklasse gleich ist, so gibt es auch eine kleinste positive Potenz von C mit einem Exponenten, der, wie leicht ersichtlich, ein Teiler von h ist, welche mit der Hauptklasse identisch wird. Man denke sich für alle Klassen diese Exponenten, zu denen sie gehören, bestimmt, nenne h_1 den größten von ihnen allen und K_1 eine der Klassen, welche zu ihm gehören; offenbar geben dann die Potenzen

$$K_1, K_1^2, K_1^3, \cdots, K_1^{h_1}$$

h_1 verschiedene Klassen. Der Exponent h', zu welchem irgend eine andere Klasse C gehört, muß ein Teiler von h_1 sein; denn entgegengesetzten Falls wäre das kleinste gemeinsame Vielfache von h_1, h' größer als h_1; indem man es aber, was stets möglich ist, gleich $\lambda_1 \cdot \lambda'$ setzt, wo λ_1, λ' relativ prim und Teiler von h_1, h' resp. sind, erhielte man im Produkte

$$K_1^{\frac{h_1}{\lambda_1}} \cdot C^{\frac{h'}{\lambda'}}$$

eine Klasse, welche leicht ersichtlich zum Exponenten $\lambda_1 \lambda' > h_1$ gehört, gegen die Bedeutung von K_1. Nun gibt es wieder für jede Klasse C eine kleinste positive Potenz, welche einer jener h_1 Potenzen von K_1 gleich wird, wenn keine andere, so doch sicherlich die Potenz $C^{h'} = K_1^{h_1} = H$; man denke sich für alle Klassen diese neuen, ihnen zugehörigen Exponenten bestimmt, nenne h_2 den größten von ihnen allen und K_2 eine der Klassen, die zu ihm gehören. Alsdann sind durch die Potenzen

$$(27) \qquad K_1^{x_1} \cdot K_2^{x_2}, \qquad \begin{pmatrix} x_1 = 1, 2, \cdots, h_1 \\ x_2 = 1, 2, \cdots, h_2 \end{pmatrix}$$

$h_1 \cdot h_2$ verschiedene Klassen bezeichnet, denn aus

$$K_1^{x_1} \cdot K_2^{x_2} = K_1^{y_1} \cdot K_2^{y_2},$$

wo auch y_1, y_2 den für x_1, x_2 angegebenen Wertreihen angehören, ergäbe sich eine Gleichung von der Form

$$K_1^{x_1 - y_1} = K_2^{y_2 - x_2},$$

aus welcher, da $y_2 - x_2$ als nicht negativ und kleiner als h_2 gedacht werden darf, notwendig $y_2 = x_2$ und darauf dann $y_1 = x_1$ erschlossen wird. Ferner erkennt man ganz ähnlich wie zuvor, daß die neuen Exponenten, zu denen irgend eine Klasse gehört, sämtlich Teiler von h_2 sein müssen. In gleicher Weise gibt es wieder für jede Klasse C eine kleinste positive Potenz, welche einem der Produkte (27) gleich wird; und wenn man sich für alle Klassen diese kleinsten Potenzen bestimmt denkt und bezeichnet mit h_3 den größten ihrer Exponenten und mit K_3 eine der zu ihm gehörigen Klassen, so liefern die Produkte

$$(28) \qquad K_1^{x_1} K_2^{x_2} K_3^{x_3}, \qquad \begin{pmatrix} x_1 = 1, 2, \cdots, h_1 \\ x_2 = 1, 2, \cdots, h_2 \\ x_3 = 1, 2, \cdots, h_3 \end{pmatrix}$$

$h_1 \cdot h_2 \cdot h_3$ verschiedene Klassen, und die jetzigen Exponenten, zu denen die einzelnen Klassen gehören, müssen Teiler sein von h_3. U. s. w. fort. Schließlich ersieht man, daß gewisse Klassen $K_1, K_2, \cdots, K_\sigma$ vorhanden sind von der Beschaffenheit, daß jede Idealklasse und jede von ihnen einmal durch das Produkt

$$K_1^{x_1} \cdot K_2^{x_2} \cdot K_3^{x_3} \cdots K_\sigma^{x_\sigma} \tag{29}$$

gegeben wird, wenn in diesem $x_1, x_2, \cdots, x_\sigma$ den ganzen Zahlen bis $h_1, h_2, \cdots, h_\sigma$ resp. gleichgesetzt werden, wo $h_1, h_2, \cdots, h_\sigma$ gewisse positive ganze Zahlen bedeuten.

Nun ist so, wie die Klassen $K_1, K_2, \cdots, K_\sigma$ bestimmt worden sind,

$$K_i^{h_i} = K_{i-1}^{a_{i-1}} \cdot K_{i-2}^{a_{i-2}} \cdots K_1^{a_1}, \tag{30}$$

wo $a_{i-1}, a_{i-2}, \cdots, a_1$ positive ganze Zahlen oder Null sind. Da ferner $K_{i-1}^{h_{i-1}}$ als ein Produkt der Klassen $K_{i-2}, \cdots, K_1$ darstellbar ist und der Exponent der niedrigsten Potenz einer Klasse, welche dies ebenfalls ist, ein Teiler von h_{i-1}, mithin die h_{i-1}^{te} Potenz jeder Klasse gleichfalls ein Produkt der Klassen $K_{i-2}, \cdots, K_1$ ist, so gilt dies auch von $K_i^{h_{i-1}}$. Daher ist h_i ein Teiler von h_{i-1}, da sonst $h_{i-1} = h_i q + r$, $0 < r < h_i$ gesetzt und aus

$$K_i^{h_{i-1}} = (K_i^{h_i})^q \cdot K_i^r$$

wegen (30) schon K_i^r als Produkt der Klassen $K_{i-1}, K_{i-2}, \cdots, K_1$ dargestellt werden könnte, der Bedeutung von K_i und h_i zuwider. Setzt man also $h_{i-1} = h_i l$, so ergibt sich mit Rücksicht auf das eben Gesagte aus (30), daß

$$K_{i-1}^{l \cdot a_{i-1}}$$

ein Produkt der Klassen $K_{i-2}, \cdots, K_1$ und folglich $l \cdot a_{i-1}$ durch $h_{i-1} = l \cdot h_i$, d. h. a_{i-1} durch h_i teilbar, $a_{i-1} = h_i c_i$ sein muß. Indem man daher

$$C_i = K_i K_{i-1}^{-c_i} \tag{31}$$

setzt, geht aus (30) die Beziehung

$$C_i^{h_i} = K_{i-2}^{b_{i-2}} \cdot K_{i-3}^{b_{i-3}} \cdots K_1^{b_1} \tag{32}$$

hervor, wo $b_{i-2}, b_{i-3}, \cdots, b_1$ wieder positive ganze Zahlen oder Null sind, während man im Ausdrucke (29) wegen der Beziehung (31) offenbar die Klasse K_i durch C_i ersetzen kann,

ohne daß er aufhören wird, alle Klassen darzustellen, wenn die x_i die angegebenen Werte durchlaufen, denn aus (31) leuchtet ein, daß C_i zu dem gleichen Exponenten h_i gehören wird wie K_i. An den Ausdruck (32) lassen sich aber ganz analoge Folgerungen knüpfen, wie sie für den Ausdruck (30) entwickelt worden sind, und wenn man in gleicher Weise fortfährt, so erkennt man, daß die Klasse K_i durch eine andere A_i ersetzt werden darf, für welche $A_i^{h_i}$ der Hauptklasse gleich:

$$A_i^{h_i} = H$$

ist. Und somit ergibt sich der folgende, oben gemeinte Satz:

Es gibt gewisse Fundamentalklassen $A_1, A_2, \cdots, A_\sigma$ von der Beschaffenheit, daß allgemein $A_i^{h_i}$ der Hauptklasse gleich ist, während jede Idealklasse und jede von ihnen auch nur einmal durch das Produkt

$$(33) \qquad C = A_1^{x_1} A_2^{x_2} \cdots A_\sigma^{x_\sigma}$$

gegeben wird, wenn darin die Exponenten x_i die Zahlen $1, 2, \cdots, h_i$ resp. durchlaufen; die Exponenten $h_1, h_2, \cdots, h_\sigma$ sind positive ganze Zahlen, deren jede (wie nach dem oben Bemerkten hinzugefügt werden darf) ein Teiler der vorhergehenden ist, und die gesamte Anzahl der Idealklassen ist

$$(33^a) \qquad h = h_1 h_2 \cdots h_\sigma.$$

Die eindeutige Darstellung aller Idealklassen durch den Ausdruck (33), welche dieser Satz liefert, läßt sich jedoch durch eine andere ersetzen, welche ihre besonderen Vorzüge hat. Man denke sich den Exponenten h_i in seine Primzahlpotenzen zerlegt, die $p', p'', \cdots$ genannt werden mögen:

$$(34) \qquad h_i = p' p'' p''' \cdots.$$

Dann können bekanntlich in eindeutiger Weise ganze Zahlen $a, a', a'', a''', \cdots$ so angegeben werden, daß

$$\frac{1}{h_i} = a + \frac{a'}{p'} + \frac{a''}{p''} + \frac{a'''}{p'''} + \cdots, \quad 0 < a^{(i)} < p^{(i)}$$

wird. Dadurch geht $A_i^{x_i}$ über in das Produkt

$$A_i^{x_i} = \left(A_i^{\frac{h_i}{p'}}\right)^{a' x_i} \cdot \left(A_i^{\frac{h_i}{p''}}\right)^{a'' x_i} \cdots$$

oder, falls zur Abkürzung

$$A_i^{\frac{h_i}{p'}} = B_i', \; A_i^{\frac{h_i}{p''}} = B_i'', \cdots$$

gesetzt wird,

$$A_i^{x_i} = B_i'^{a'x_i} \cdot B_i''^{a''x_i} \cdots,$$

wo nun die einzelnen Klassen $B_i', B_i'', \cdots$ den Gleichungen

$$B_i'^{p'} = H, \quad B_i''^{p''} = H, \cdots$$

genügen, deren Grade Primzahlen oder Primzahlpotenzen sind. Verfährt man in dieser Weise mit jeder der Fundamentalklassen A_i, so kann schließlich jede Idealklasse in eindeutiger Weise durch eine Reihe von neuen Fundamentalklassen dargestellt werden, welche zu Exponenten gehören, die Primzahlen oder Primzahlpotenzen sind, d. h. welche der Hauptklasse gleich werden, wenn sie zu Potenzen mit diesen Exponenten erhoben werden. Es verdient indessen bemerkt zu werden, daß, wenn die Exponenten, zu denen die Fundamentalklassen gehören, auf solche Weise an Einfachheit gewinnen, sie andererseits der charakteristischen Eigenschaft der Exponenten h_i verlustig gehen, daß jeder von ihnen ein Teiler des vorhergehenden ist. Jedoch zeigen die Formeln (33ᵃ) und (34), daß auch jetzt das Produkt aller Exponenten, zu denen die neuen Fundamentalklassen gehören, gleich der Gesamtanzahl der Idealklassen bleibt.

6. Die Anzahl der Idealklassen eines beliebigen Körpers ist das völlige Analogon zur Anzahl der Klassen äquivalenter quadratischer Formen. Es lag daher nahe, die analytische Methode, durch welche es Dirichlet gelungen ist, die letztere zu ermitteln, auch auf das entsprechende allgemeinere Problem der Bestimmung der Idealklassenanzahl zur Anwendung zu bringen. Dedekind hat dies getan und auf solchem Wege die gesuchte Anzahl allgemein wenigstens soweit bestimmt, als zur Zeit es möglich erscheint. Wir folgen seinem Vorgange, indem wir vor allem folgenden Satz beweisen:

Ist $\mathfrak{j}$ ein gegebenes Körperideal und t eine positive unendlich wachsende Größe, T aber die Anzahl aller verschiedenen durch $\mathfrak{j}$ teilbaren Hauptideale, deren Normen nicht größer sind als der jedesmalige Wert von t, so ist

$$(35)\qquad \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot Q}{\mathfrak{N}(\mathfrak{j}) \cdot \sqrt{(D)}},$$

wenn (D) den numerischen Wert der Grundzahl D und

$$(36)\qquad Q = \frac{|l_k(E_i)|}{\varrho}$$

den Quotienten aus dem Regulator eines Systems von Fundamentaleinheiten und der Anzahl der im Körper enthaltenen Einheitswurzeln, σ aber Null oder Eins bedeutet, je nachdem $n = 2s$ ist oder nicht. Hierbei verstehen wir unter einem Hauptideale jedes Ideal $\mathfrak{g}\alpha$, für welches $N(\alpha)$ einen positiven Wert hat, und dementsprechend unter einer „Einheit" nur diejenigen ganzen Zahlen ε, deren Norm $+1$ ist. Ein solches Hauptideal wird dann und nur dann durch $\mathfrak{j}$ teilbar, d. i. in $\mathfrak{j}$ enthalten sein, wenn α selbst eine Zahl des Ideals $\mathfrak{j}$, also

$$(37)\qquad \alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

ist, vorausgesetzt, daß $\alpha_1, \alpha_2, \cdots, \alpha_n$ irgend eine Basis des Ideals $\mathfrak{j}$ bezeichnen. Man erhält daher gewiß sämtliche im Satze angegebenen Hauptideale $\mathfrak{g}\alpha$, wenn man die Koeffizienten a_i in der Formel (37) so wählt, daß

$$(38)\qquad 0 < N(\alpha) < t$$

wird. Aber die so erhaltenen Hauptideale sind nicht sämtlich voneinander verschieden. Zwei von ihnen, $\mathfrak{g}\alpha$, $\mathfrak{g}\alpha'$ können einander nur gleich sein, wenn α, α' einander eigentlich assoziiert, d. h. um einen Faktor ε verschieden sind, der eine Einheit ist mit positiver Norm; ist aber α eine Zahl in $\mathfrak{j}$ und ε irgend eine Einheit mit positiver Norm, so gehört auch $\varepsilon\alpha$ dem Ideale $\mathfrak{j}$ an, die Hauptideale $\mathfrak{g}\alpha$ und $\mathfrak{g}\varepsilon\alpha$ sind mit einander identisch und $N(\varepsilon\alpha)$ ist gleich $N(\alpha)$. Jedes der gedachten Hauptideale tritt also unendlich oft auf. Bezeichnet man jedoch, wie in Nr. 9 des vorigen Kapitels, mit $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ irgend ein System von $s-1$ unabhängigen Einheiten mit positiver Norm und mit η jede der in bezug auf dieses System reduzierten Einheiten mit der Norm $+1$, deren Anzahl ϱ_0 heiße, so zerfällt die Menge aller mit α eigentlich assoziierten Zahlen in ϱ_0 Komplexe von der Form

$$\alpha \cdot \eta \varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_{s-1}^{m_s-1}$$

und in jedem derselben gibt es, wie a. a. O. gezeigt, eine einzige reduzierte Zahl, welche der Einfachheit wieder α heiße, d. i. eine Zahl α von der Beschaffenheit, daß in den Gleichungen

$$(39) \qquad e_1 \cdot l_{i1} + e_2 \cdot l_{i2} + \cdots + e_{s-1} l_{i,s-1} + f \cdot c_i = l_i(\alpha) \qquad (i = 1, 2, \cdots, s)$$

die sogenannten Exponenten $e_i(\alpha)$ oder e_i zwischen 0 und 1 liegen, in Zeichen:

$$(40) \qquad 0 < e_i(\alpha) < 1. \qquad (i = 1, 2, \cdots, s-1)$$

Fügt man daher den Bedingungen (37) und (38) noch diese neue Bedingung (40) hinzu, so erhält man jedes der gewollten Hauptideale $\mathfrak{g}\alpha$ genau ϱ_0 Mal, oder die Anzahl aller durch jene drei Bedingungen bestimmten ganzen Zahlen α beträgt $\varrho_0 \cdot T$.

Dies vorausgeschickt, seien $\alpha_i^{(1)}, \alpha_i^{(2)}, \cdots, \alpha_i^{(n)}$ die zu α_i konjugierten Werte und

$$(41) \qquad \begin{aligned} w^{(1)} &= u_1 \alpha_1^{(1)} + u_2 \alpha_2^{(1)} \cdots + u_n \alpha_n^{(1)} \\ w^{(2)} &= u_1 \alpha_1^{(2)} + u_2 \alpha_2^{(2)} \cdots + u_n \alpha_n^{(2)} \\ &\cdots\cdots\cdots\cdots \\ w^{(n)} &= u_1 \alpha_1^{(n)} + u_2 \alpha_2^{(n)} + \cdots + u_n \alpha_n^{(n)} \end{aligned}$$

die dem Ideale $\mathfrak{j}$ entsprechende Linearform w und deren Konjugierte. Jedem reellen Systeme der Unbestimmten u_i entspricht ein eindeutig bestimmtes System $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$. Wird aber ferner für $i = 1, 2, \cdots, s$ der reelle Bestandteil des Ausdrucks $c_i \log w^{(i)}$ mit y_i bezeichnet, und

$$(42) \qquad z_1 l_{i1} + z_2 l_{i2} + \cdots + z_{s-1} l_{i,s-1} + v \cdot c_i = y_i \qquad (i = 1, 2, \cdots, s)$$

gesetzt, so sind auf solche Weise mit den u_i zugleich nicht nur die y_i, sondern auch die z_i und die Größe v als reelle Größen eindeutig definiert. Aus den Beziehungen (42) folgt, wenn

$$(43) \qquad \text{abs. } N(w) = u$$

gesetzt wird, bei Beachtung der Formeln (20) und (22) des vorigen Kapitels noch die folgende:

$$(44) \qquad nv = y_1 + y_2 + \cdots + y_s = \log u.$$

Die Gesamtheit aller reellen Wertsysteme $u_1, u_2, \cdots, u_n$ bildet ein n-fach unbegrenztes Gebiet. Wenn wir diese Wertsysteme aber durch die den Ungleichheiten (38) und (40) nachgebildeten Bedingungen

$$(45) \qquad 0 < u \overline{\gtrless} 1$$

$$(46) \qquad 0 \overline{\overline{\gtrless}} z_i < 1 \quad (i = 1, 2, \cdots, s-1)$$

beschränken, so stellen wir nicht nur völlige Analogie mit den auf die Zahlen α bezüglichen Beziehungen her, sondern bestimmen auch für die u_i ein endlich begrenztes Gebiet, welches $\mathfrak{A}$ genannt werde. In der Tat können der letzten Bedingungen wegen mit Rücksicht auf (44) die durch die Gleichungen (42) bestimmten reellen Größen y_i endliche, nur von dem Systeme der unabhängigen Einheiten bestimmte Grenzen nicht überschreiten, woraus dasselbe für die absoluten Beträge der $w^{(i)}$ und deshalb nach den Gleichungen (41), deren Determinante von Null verschieden ist, auch für diejenigen der Unbestimmten u_i erschlossen wird.

Offenbar besteht nun zwischen der Gesamtheit der dem Gebiete $\mathfrak{A}$ angehörigen Systeme der Unbestimmten u_i und der Gesamtheit der vorher besprochenen ganzen Zahlen α ein naher Zusammenhang, den es klarzustellen gilt. Setzt man zur Abkürzung

$$(47) \qquad \delta = \frac{1}{t^{\frac{1}{n}}}$$

und wählt das Wertsystem

$$(48) \qquad u_1 = \delta a_1, \ u_2 = \delta a_2, \ \cdots, \ u_n = \delta a_n,$$

so gehen $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$ in die δ-fachen der Zahl α und ihrer konjugierten Zahlen über, infolge davon wird $N(w) = \frac{1}{t} N(\alpha)$, ferner

$$y_i = c_i \log w^{(i)} = c_i \log \delta + l_i(\alpha),$$

d. h.

$$y_i = e_1(\alpha) \cdot l_{i1} + \cdots + e_{s-1}(\alpha) \cdot l_{i,s-1} + c_i(f + \log \delta) \quad (i = 1, 2, \cdots, s)$$

aus welchen Gleichungen, wenn sie mit den Gleichungen (42) verglichen werden, die anderen:

$$z_i = e_i(\alpha),\ v = f + \log \delta$$

hervorgehen. Da nun für die Zahl α die Ungleichheiten (38) und (40) bestehen, so ergeben sich für das gewählte Wertsystem (48) der u_i die Ungleichheiten (45) und (46), d. h. jeder der Zahlen α entspricht ein im Innern des Gebietes $\mathfrak{A}$ gelegenes System der Unbestimmten u_i von der Form (48), nämlich ein Wertsystem, welches durch δ geteilt zu einem ganzzahligen wird. Umgekehrt aber wird auch jedem solchen innerhalb $\mathfrak{A}$ gelegenen Wertsysteme der u_i eine jener Zahlen α zugeordnet sein, da aus den für die u_i geltenden Bedingungen, wenn die Gleichungen (48) statthaben, sich eine durch die aus den letzteren folgenden Zahlen a_i bestimmte Zahl α ergibt, welche den Bedingungen (37) bis (40) genügt. Man erkennt also hiernach, daß die Anzahl der gedachten Zahlen α derjenigen der in $\mathfrak{A}$ gelegenen Systeme der u_i von der Form (48) gleich, nämlich jede von ihnen gleich $\varrho_0 T$ ist.

Hier erinnern wir an einen allgemeinen Satz über vielfache bestimmte Integrale, den zuerst Dirichlet in seinen analytisch-zahlentheoretischen Untersuchungen benutzt hat und der in des Verfassers „Analytischer Zahlentheorie", 6. Abschnitt, Nr. 1 und 13. Abschnitt, Nr. 10 entwickelt worden ist (eingehender in H. Webers Algebra II, § 184):

Das aus lauter positiven Elementen bestehende, über das endliche Gebiet $\mathfrak{A}$ ausgedehnte Integral

$$\int du_1 \cdot du_2 \cdots du_n$$

kann als der Grenzwert des Produkts aus der Anzahl aller im Innern von $\mathfrak{A}$ gelegenen Systeme der u_i von der Form (48) und der Potenz δ^n aufgefaßt werden für den Fall, daß δ unendlich klein wird, indem bei diesem Grenzübergange die Werte u_i, wenn die a_i um Einheiten sich ändern, nur um ihre Differenziale veränderlich werden. In unserm Falle findet sich somit

$$\int du_1 \cdot du_2 \cdots du_n = \lim_{\delta = 0} (\varrho_0 T \cdot \delta^n)$$

oder, was dasselbe sagt,

$$(49)\qquad \int du_1 \cdot du_2 \cdots du_n = \varrho_0 \cdot \lim_{t=\infty} \left(\frac{T}{t}\right) \cdot$$

Der Wert dieses n-fachen Integrales berechnet sich durch eine Reihe von Transformationen der Variabeln und ergibt dann leicht die Formel (35). Führen wir zunächst statt der u_i durch die eindeutige Substitution (41) die n andern Variabeln $w^{(1)}$, $w^{(2)}, \cdots, w^{(n)}$ ein, für welche Substitution die Funktionaldeterminante

$$\left|\frac{\partial u_i}{\partial (w^{(k)})}\right| = \frac{1}{\left|\frac{\partial (w^{(k)})}{\partial u_i}\right|} = \frac{1}{\sqrt{\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)}}$$

gefunden wird, so ergibt sich das Integral gleich

$$(50) \qquad \frac{1}{\sqrt{\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)}} \cdot \int dw^{(1)} \cdot dw^{(2)} \cdots dw^{(n)}.$$

Werden nun statt der $n = r + 2q$ Größen $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$ die $s = r + q$ Größen y_i, d. h. die reellen Bestandteile der Logarithmen

$$\log w^{(1)}, \log w^{(2)}, \cdots, \log w^{(r)}, 2 \log w^{(r+1)}, \cdots, 2 \log w^{(r+q)},$$

von denen die letzten q zu den Logarithmen

$$2 \log w^{(r+q+1)}, \cdots, 2 \log w^{(r+2q)}$$

konjugiert imaginär sind, eingeführt, so bedarf es, um die Größen $w^{(i)}$ völlig zu bestimmen, noch der imaginären Bestandteile dieser Logarithmen; wir bezeichnen dieselben mit $i \cdot \varphi_1, i \cdot \varphi_2, \cdots, i \cdot \varphi_{r+q}$, indem wir die Bögen $\varphi_1, \varphi_2 \cdots, \varphi_{r+q}$ der Bestimmtheit wegen nicht negativ und kleiner als 2π wählen; die ersten r von ihnen werden dann, da $w^{(1)}, w^{(2)}, \cdots, w^{(r)}$ reell sind, Null oder π sein. Auf solche Weise entspricht jedem Systeme $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$ ein bestimmtes Wertsystem der Größen $y_1, y_2, \cdots, y_{r+q}, \varphi_1, \varphi_2, \cdots, \varphi_{r+q}$, wie auch umgekehrt. Werden dagegen nur die n Größen

$$(51) \qquad y_1, y_2, \cdots, y_{r+q}, \varphi_{r+1}, \varphi_{r+2}, \cdots, \varphi_{r+q}$$

gegeben, so sind dadurch zwar auch die Größen $w^{(r+1)}, w^{(r+2)}, \cdots, w^{(r+q)}, \cdots, w^{(n)}$ völlig mitbestimmt, dagegen die ersten r Größen $w^{(1)}, w^{(2)}, \cdots, w^{(r)}$ nur bis auf ihr Vorzeichen, welches unbestimmt bleibt, und somit entspricht jedem Wertsysteme der Größen (51) nicht ein, sondern genau 2^r verschiedene Wertsysteme der Größen $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$. Indessen ist, da das

Produkt dieser Größen, nämlich u, nach (45) positiv sein soll, von diesen Systemen nur die Hälfte, also nur die Anzahl 2^{r-1} derselben zulässig, wenn $r > 0$, d. h. wenn nicht $n = 2s$ ist. Da nun den Größen $y_1, y_2, \cdots, y_{r+q}$ wieder die Größen $z_1, z_2, \cdots, z_{r+q-1}, v$ oder auch $z_1, z_2, \cdots, z_{r+q-1}, u$ durch die Beziehungen (42) und (44) eindeutig zugeordnet sind, so darf man sagen: jedem Wertsysteme

(52) $$z_1, z_2, \cdots, z_{r+q-1}, u, \varphi_{r+1}, \varphi_{r+2}, \cdots, \varphi_{r+q},$$

welches den Bedingungen (45) und (46), sowie den Ungleichheiten

(53) $$0 \leqq \varphi_{r+i} < 2\pi \quad (i = 1, 2, \cdots, q)$$

genügt, entsprechen, je nachdem $n = 2s$ ist oder nicht, genau 2^r, bezw. 2^{r-1} im Integrale (50) auftretende Wertsysteme $w^{(1)}, w^{(2)}, \cdots, w^{(n)}$. Nun findet sich zunächst

für $i = 1, 2, \cdots, r$: $$dw^{(i)} = w^{(i)} \cdot dy_i$$

für $i = r+1, r+2, \cdots, r+q$: $$\begin{cases} dw^{(i)} = \dfrac{w^{(i)}}{2} \cdot dy_i + w^{(i)} \cdot \sqrt{-1} \cdot d\varphi_i \\ dw^{(r+i)} = \dfrac{w^{(r+i)}}{2} \cdot dy_i - w^{(r+i)} \cdot \sqrt{-1} \cdot d\varphi_i, \end{cases}$$

wodurch die Funktionaldeterminante der $w^{(i)}$ in bezug auf die Größen (51) den Wert

(54) $$N(w) \cdot (-\sqrt{-1})^q = \pm u \cdot (\sqrt{-1})^q$$

erhält. Ferner ist den Gleichungen (42) zufolge

$$dy_i = l_{i1} dz_1 + l_{i2} dz_2 + \cdots + l_{i,s-1} dz_{s-1} + c_i dv \quad (i = 1, 2, \cdots, r+q)$$

und daher die Funktionaldeterminante der Größen (51) in bezug auf die Größen

$$z_1, z_2, \cdots, z_{r+q-1}, v, \varphi_{r+1}, \cdots, \varphi_{r+q}$$

gleich der Determinante (49) des vorigen Kapitels, d. i. gleich

(55) $$n \cdot | l_k(\varepsilon_i) |.$$

Da endlich nach (44)

(56) $$dv = \frac{1}{nu} \cdot du$$

ist, so ergibt sich aus (54), (55), (56) durch Zusammensetzung das Resultat:

Jedes Element des Integrales (50) hat den Wert

$$\pm u \cdot (\sqrt{-1})^q \cdot n \cdot |l_k(\varepsilon_i)| \cdot \frac{1}{nu} \cdot dz_1 \cdots dz_{r+q-1} \cdot du \cdot d\varphi_{r+1} \cdots d\varphi_{r+q}$$
$$= \pm (\sqrt{-1})^q \cdot |l_k(\varepsilon_i)| \cdot dz_1 \cdots dz_{r+q-1} \cdot du \cdot d\varphi_{r+1} \cdots d\varphi_{r+q},$$

und dieser selbe Wert tritt dem oben Gesagten zufolge genau $2^{r-\sigma}$ mal auf. Demnach geht der Ausdruck (50) in den folgenden über:

$$\pm (\sqrt{-1})^q \cdot \frac{2^{r-\sigma} \, |l_k(\varepsilon_i)|}{\sqrt{\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)}} \cdot \int dz_1 \cdots dz_{r+q-1} \cdot du \cdot d\varphi_{r+1} \cdots d\varphi_{r+q},$$

in welchem die Integrationen in bezug auf die einzelnen Variabeln voneinander unabhängig und durch die Ungleichheiten (45), (46) und (53) bestimmt sind. Er findet sich also gleich

$$\pm (\sqrt{-1})^q \cdot \frac{2^{r-\sigma} \cdot (2\pi)^q \cdot |l_k(\varepsilon_i)|}{\sqrt{\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)}},$$

wo das Vorzeichen so zu wählen ist, daß der Ausdruck positiv wird. Nun ist aber die Diskriminante des Ideals $\mathfrak{j}$ nach Formel (51) des ersten und Formel (46) des vierten Kapitels gleich $\mathfrak{N}(\mathfrak{j})^2 \cdot \mathrm{D}$ und das Vorzeichen von D dasjenige von $(-1)^q$, und so gelangen wir schließlich, zur Gleichung (49) zurückgreifend, zu dem Ergebnisse, daß der Grenzwert

$$\lim_{t=\infty} \cdot \left(\frac{T}{t}\right)$$

gleich dem Ausdrucke

$$\frac{2^{s-\sigma} \cdot \pi^q}{\mathfrak{N}(\mathfrak{j}) \cdot \sqrt{(\mathrm{D})}} \cdot \frac{|l_k(\varepsilon_i)|}{\varrho_0}$$

ist.

Der gefundene Ausdruck für $\lim\limits_{t=\infty} \left(\frac{T}{t}\right)$ besteht, wie man sieht, aus zwei Faktoren, von denen der erste nur von der Natur des der Betrachtung zum Grunde liegenden Körpers abhängig, der zweite dagegen durch das willkürlich gewählte System unabhängiger Einheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ bestimmt ist. Da aber der gesamte Ausdruck nach seiner Bedeutung von dieser willkürlichen Auswahl unabhängig sein muß, da er nur

vom Körper selbst bestimmt wird, so ergibt sich die bemerkenswerte Folgerung, daß der Quotient

$$\frac{|l_k(\varepsilon_i)|}{\varrho_0}$$

zwischen dem Regulator eines Systems von $s-1$ unabhängigen Einheiten und der Anzahl der mit bezug auf dasselbe reduzierten Einheiten für jedes System der gleiche ist. Aus diesem Grunde darf für diesen Quotienten der auf ein System von Fundamentaleinheiten bezügliche

$$\frac{|l_k(E_i)|}{\varrho}$$

gesetzt werden, und so gelangt man schließlich zur behaupteten Formel (35).

Auf Grund derselben ist nun leicht die Wahrheit dieses anderen Satzes zu erkennen:

Ist C irgend eine Idealklasse (wobei zur Verteilung der Ideale in Klassen der engere Äquivalenzbegriff der Nr. 3 maßgebend sein soll) und T die Anzahl verschiedener in C enthaltenen Ideale, deren Norm nicht größer ist als die positive Größe t, so findet sich

$$\lim_{t=\infty}\left(\frac{T}{t}\right)=\frac{2^{s-\sigma}\cdot\pi^{n-s}\cdot Q}{\sqrt{(\mathrm{D})}}. \tag{57}$$

Bezeichnet nämlich $\mathfrak{j}$ ein beliebig gewähltes Ideal der inversen Klasse C' und $\mathfrak{a}$ die verschiedenen Ideale der Klasse C, so sind die sämtlichen Produkte $\mathfrak{j}\cdot\mathfrak{a}$ voneinander verschiedene Hauptideale $\mathfrak{g}\alpha$, welche durch $\mathfrak{j}$ teilbar sind, und umgekehrt hat jedes Hauptideal dieser Art die Form eines Produkts $\mathfrak{j}\cdot\mathfrak{a}$, wo der Faktor $\mathfrak{a}$ ein Ideal der zu C' entgegengesetzten Klasse C sein muß. Indem also $\mathfrak{a}$ alle diese Ideale durchläuft, durchläuft $\mathfrak{j}\cdot\mathfrak{a}$ die verschiedenen durch $\mathfrak{j}$ teilbaren Hauptideale, und, da

$$\mathfrak{N}(\mathfrak{j}\mathfrak{a})=\mathfrak{N}(\mathfrak{j})\cdot\mathfrak{N}(\mathfrak{a})$$

ist, werden denjenigen der Ideale $\mathfrak{a}$, deren Norm nicht größer ist als t, diejenigen durch $\mathfrak{j}$ teilbaren Hauptideale entsprechen, deren Normen nicht größer sind als $t\cdot\mathfrak{N}(\mathfrak{j})$; die Anzahl T im ausgesprochenen Satze bedeutet somit auch die Anzahl dieser letztbezeichneten Hauptideale. Setzt man aber in der Formel

(35) an Stelle von t die Größe $t \cdot \mathfrak{N}(\mathfrak{j})$, so ergibt sich durch Hebung des Faktors $\mathfrak{N}(\mathfrak{j})$ die Gleichung

$$\lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot Q}{\sqrt{(\mathrm{D})}},$$

wie sie behauptet worden ist.

Da der so gefundene auf eine beliebige Idealklasse C bezügliche Grenzwert allein vom Körper selbst bestimmt ist, nämlich nichts enthält, was der besonderen Klasse charakteristisch wäre, ist er für jede dieser Klassen ein- und derselbe. Wenn daher jetzt unter T nicht die Anzahl derjenigen in einer bestimmten *Klasse* enthaltenen, sondern derjenigen Ideale *überhaupt* verstanden wird, deren Normen nicht größer sind als eine positive Größe t, so erhält man endlich nachstehende Formel:

$$(58) \qquad \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot Q}{\sqrt{(\mathrm{D})}} \cdot h,$$

welche die Grundlage bildet zur Bestimmung der Klassenanzahl h.

7. Hierbei kann nach einem sehr allgemeinen Dirichletschen Satze (s. Analytische Zahlentheorie, 3. Abschnitt, Nr. 8) der Grenzwert zur Linken der vorigen Formel durch einen andern ersetzt werden. Wenn nämlich die nach der steigenden Größe der Normen geordnete, über alle verschiedenen Ideale $\mathfrak{j}$ des Körpers ausgedehnte Summe[1])

$$(59) \qquad \sum_{\mathfrak{j}} \frac{1}{\mathfrak{N}(\mathfrak{j})^{\lambda}} = Z(\lambda)$$

(für $\lambda > 1$) gesetzt wird, so besteht jenem Satze zufolge die Gleichheit

$$(60) \qquad \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \lim_{\lambda=1} \cdot (\lambda - 1)\, Z(\lambda).$$

Wir leiten diese Formel folgendermaßen her.

Bezeichnet man mit $F(\nu)$ die Anzahl der verschiedenen

---

1) Über die analytische Natur dieser Funktion von λ s. Landau, über die zu einem algebraischen Zahlkörper gehörige Zetafunktion, Journ. f. Math. 125, p. 63. Beachte auch Dess. Arbeit ebend. 127, p. 167.

Ideale des Körpers, deren Norm ν ist, so ist für jeden ganzzahligen Wert ν der positiven Größe t

$$\frac{T}{t} = \frac{F(1) + F(2) + \cdots + F(\nu)}{\nu}$$

und somit auch

$$(61) \qquad \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \lim_{\nu=\infty} \cdot \frac{F(1) + F(2) + \cdots + F(\nu)}{\nu}.$$

Man denke sich nun die sämtlichen verschiedenen Ideale

$$\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \cdots, \mathfrak{j}_i, \cdots$$

nach der Größe ihrer Normen

$$N_1, N_2, N_3, \cdots, N_i, \cdots$$

geordnet, sodaß allgemein $N_i \overline{\gtrless} N_{i-1}$ ist. Setzt man dann $\nu = N_i$, so ist die Anzahl derjenigen Ideale, deren Norm $\overline{<} \nu$ ist, mindestens i, da noch unter den auf $\mathfrak{j}_i$ folgenden Idealen einige sein können, deren Norm gleich ν ist; andererseits muß die Anzahl der Ideale, deren Norm $\overline{\lessgtr} \nu - 1$ ist, kleiner als i sein, da wenigstens das Ideal $\mathfrak{j}_i$ eine schon größere Norm hat. So finden sich die beiden Ungleichheiten:

$$F(1) + F(2) + \cdots + F(\nu - 1) < i \overline{\lessgtr} F(1) + F(2) + \cdots + F(\nu),$$

denen man die Form geben kann

$$\frac{F(1) + F(2) + \cdots + F(\nu-1)}{\nu - 1} \cdot \left(1 - \frac{1}{\nu}\right) < \frac{i}{N_i} \overline{\lessgtr} \frac{F(1) + F(2) + \cdots + F(\nu)}{\nu}.$$

Setzt man nun zur Abkürzung

$$(62) \qquad \frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot Q}{\sqrt{(\mathrm{D})}} = g,$$

so ergibt sich aus den Ungleichheiten mit Rücksicht auf (58) und (61) für ein unendlich wachsendes $\nu = N_i$ oder i die Gleichung

$$\lim_{i=\infty} \frac{i}{N_i} = gh,$$

d. h. man kann bei einem beliebig kleinen δ für i einen so großen Wert i' wählen, daß für jedes $i \overline{\gtrless} i'$

$$(63) \qquad \frac{gh - \delta}{i} < \frac{1}{N_i} < \frac{gh + \delta}{i}$$

bleibt. Nun ist, wenn $\lambda > 1$,

$$Z(\lambda) = \sum_{\mathfrak{j}} \frac{1}{\mathfrak{N}(\mathfrak{j})^{\lambda}} = \sum_{i} \frac{1}{N_i^{\lambda}}$$

gesetzt, und aus den letzten Ungleichheiten ergibt sich das folgende andere Paar:

$$(gh - \delta)^{\lambda} \cdot (\lambda - 1) \sum_{i=i'}^{\infty} \frac{1}{i^{\lambda}} < (\lambda - 1) \cdot \sum_{i=i'}^{\infty} \frac{1}{N_i^{\lambda}}$$

$$< (gh + \delta)^{\lambda} \cdot (\lambda - 1) \sum_{i=i}^{\infty} \frac{1}{i^{\lambda}},$$

mithin aus der bekannten Konvergenz der Reihe

$$\sum_{i=i'}^{\infty} \frac{1}{i^{\lambda}}$$

für $\lambda > 1$ unter der gleichen Bedingung auch diejenige der Reihe $Z(\lambda)$. Zudem ist, wie bekannt,

$$\lim_{\lambda=1} \cdot (\lambda - 1) \sum_{i=1}^{\infty} \frac{1}{i^{\lambda}} = \lim_{\lambda=1} \cdot (\lambda - 1) \sum_{i=i'}^{\infty} \frac{1}{i^{\lambda}} = 1,$$

man folgert also aus den letzten Ungleichheiten durch den Übergang zur Grenze $\lambda = 1$ die folgenden:

$$gh - \delta < \lim_{\lambda=1} \cdot (\lambda - 1) Z(\lambda) < gh + \delta$$

oder, da hier δ beliebig klein gedacht werden darf, die Gleichheit

$$\lim_{\lambda=1} \cdot (\lambda - 1) Z(\lambda) = gh,$$

welche vermöge (58) mit (60) identisch ist.

Demnach darf man setzen

$$h = \frac{1}{g} \lim_{\lambda=1} \cdot (\lambda - 1) \sum_{\mathfrak{j}} \frac{1}{\mathfrak{N}(\mathfrak{j})^{\lambda}}, \tag{64}$$

wodurch die Anzahl der Idealklassen als Grenzwert einer aus den Normen sämtlicher Ideale des Körpers zusammengesetzten unendlichen Reihe bestimmt wird.

Wenn nun auch auf solche Weise ein sehr bedeutender Schritt getan ist zur Ermittlung der Klassenanzahl, indem in

der gefundenen Formel ein Gesetz aufgestellt ist, wie sie für alle Körper aus der Gesamtheit ihrer Ideale abgeleitet werden kann, so bedarf es doch noch der Summierung der in der Formel enthaltenen unendlichen Reihe, welche kaum allgemein geleistet werden kann, sondern je nach der Natur des Körpers, mit welcher die analytische Beschaffenheit der Reihe jedenfalls aufs engste verknüpft ist, verschiedener Hilfsmittel bedarf. Dieser Teil der Aufgabe ist bisher erst für sehr wenige Körper gelöst worden; zu ihnen zählen die quadratischen und einige der biquadratischen Körper, desgleichen die jene umfassenden Kreisteilungskörper. Für die ersteren hat Dirichlet in seinen Untersuchungen über quadratische Formen mit reellen oder komplexen Elementen die Klassenanzahl unter endlicher Form angegeben, für die letzteren Kummer das Gleiche geleistet; Dedekind hat für kubische Körper die Aufgabe behandelt.[1]) Bei all' diesen Untersuchungen hat sich gezeigt, daß die Lösung nur aus der genauesten Kenntnis der algebraischen Eigenschaften des vorliegenden Körpers geschöpft werden kann, zudem aber auch jedesmal der Theorie gewisser Transscendenten bedarf, der Exponentialfunktion, der elliptischen oder der Modulfunktionen usw., deren Kenntnis man erst viel weiter wird vertieft haben müssen, bevor allgemeinere Resultate für den gedachten zweiten Teil der Aufgabe erhofft werden können.

8. Indem wir also hier mit der Ableitung der Formel (64) die Betrachtung dieser Aufgabe beschließen, fügen wir jedoch noch einige Resultate hinzu, die nicht ohne weiteres Interesse sind. Einmal leuchtet ein, daß die Gleichung (59) für $Z(\lambda)$ auch so geschrieben werden kann:

$$(59^{a}) \qquad Z(\lambda) = \sum_{\nu=1}^{\infty} \frac{F(\nu)}{\nu^{\lambda}}.$$

---

1) Dirichlet, recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres, Journ. f. Math. 19, p. 324; 21, p. 1 und 134; recherches sur les formes quadratiques à coefficiens et à indéterminées complexes, Journ. f. Math. 24, p. 291. S. auch Bachmann, zur Theorie der komplexen Zahlen, ebendas. 67, p. 200. Ferner Kummer, Bestimmung der Anzahl nicht äquivalenter Klassen für die aus λ^{ten} Wurzeln der Einheit gebildeten komplexen Zahlen usw., Journ. f. Math. 40, p. 93 und 117; Dedekind, über die Anzahl der Idealklassen in reinen kubischen Körpern, ebendas. 121, p. 40.

Bedenkt man aber, daß die Ideale aus den Primidealpotenzen zusammengesetzt sind, gerade wie die sämtlichen rationalen ganzen Zahlen aus den Primzahlpotenzen, so findet sich, entsprechend der bekannten Eulerschen Formel

$$\sum_{\nu=1}^{\infty} \frac{1}{\nu^{\lambda}} = \prod_{p} \frac{1}{1-\frac{1}{p^{\lambda}}}$$

die folgende dritte Ausdrucksweise der Funktion $Z(\lambda)$:

$$(59^{b}) \qquad Z(\lambda) = \prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{\mathfrak{N}(\mathfrak{p})^{\lambda}}},$$

wo die angedeutete Multiplikation sich auf sämtliche Primideale $\mathfrak{p}$ des Körpers zu erstrecken hat. Dedekind hat diesen Ausdrucksweisen noch eine vierte hinzugefügt. Da, wenn p eine rationale Primzahl bezeichnet, das Hauptideal $\mathfrak{g}p$ stets nur aus einer endlichen Anzahl von Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ zusammengesetzt ist, so findet sich p nur in diesen Primidealen, in ihnen aber auch wirklich, und jedes von ihnen hat einen bestimmten Grad $f_1, f_2, \cdots, f_r$, sodaß allgemein $\mathfrak{N}(\mathfrak{p}_i) = p^{f_i}$ ist. Faßt man daher von den Faktoren des Produkts (59^b) stets diejenigen zusammen, die sich auf die Ideale derselben Primzahl p beziehen, so läßt sich schreiben:

$$(59^{c}) \qquad Z(\lambda) = \prod_{p} \frac{1}{\left(1-\frac{1}{p^{\lambda f_1}}\right)\left(1-\frac{1}{p^{\lambda f_2}}\right)\cdots\left(1-\frac{1}{p^{\lambda f_r}}\right)},$$

während die Multiplikation sich auf sämtliche rationale Primzahlen erstreckt. Entwickelt man hier das allgemeine Glied des Produkts, so erhält man dafür die Summe aller Ausdrücke

$$\frac{1}{p^{\lambda(f_1 x_1 + f_2 x_2 + \cdots + f_r x_r)}} = \frac{1}{\mathfrak{N}(\mathfrak{p}_1^{x_1}\mathfrak{p}_2^{x_2}\cdots\mathfrak{p}_r^{x_r})^{\lambda}}$$

für ganzzahlige x_i, welche Null oder positiv sind, und wenn nun diejenigen dieser Ausdrücke vereint werden, in denen

$$f_1 x_1 + f_2 x_2 + \cdots + f_r x_r$$

den gleichen Wert μ hat, und welche demnach sämtlich gleich $\frac{1}{p^{\lambda\mu}}$ sind, so ist deren Summe, da jedes Ideal, dessen Norm p^{μ} ist, nur aus den Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$ zusammengesetzt

sein kann, nichts anderes als $\frac{F(p^\mu)}{p^{\lambda\mu}}$, demnach das allgemeine Glied des Produkts (59^c) gleich

$$1 + \frac{F(p)}{p^\lambda} + \frac{F(p^2)}{p^{2\lambda}} + \frac{F(p^3)}{p^{3\lambda}} + \cdots. \tag{65}$$

Nun hat die Funktion $F(\nu)$ die Eigenschaft, daß für relativ prime Argumente a, b

$$F(ab) = F(a) \cdot F(b) \tag{66}$$

ist. In der Tat, ist $\mathfrak{j}$ ein Ideal, für welches

$$\mathfrak{N}(\mathfrak{j}) = ab \tag{67}$$

ist, so muß, da die Norm jedes in $\mathfrak{j}$ aufgehenden Primideales $\mathfrak{p}$ nur eine Potenz einer der in a, oder einer der davon verschiedenen in b aufgehenden rationalen Primzahlen sein kann, $\mathfrak{N}(\mathfrak{p})$ in einem, aber auch nur in einem der Faktoren a, b als Teiler enthalten sein und somit $\mathfrak{j}$ sich in zwei Idealfaktoren $\mathfrak{a}$, $\mathfrak{b}$ zerlegen, deren Normen nur aus Primfaktoren von a resp. von b zusammengesetzt sind; und da

$$ab = \mathfrak{N}(\mathfrak{j}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b})$$

ist, muß notwendig

$$\mathfrak{N}(\mathfrak{a}) = a, \; \mathfrak{N}(\mathfrak{b}) = b$$

sein. Also entspricht jedem Ideale $\mathfrak{j}$ mit der Norm ab ein Paar von Idealen $\mathfrak{a}$, $\mathfrak{b}$ mit den Normen a, b resp.; die Anzahl solcher Paare ist $F(a) \cdot F(b)$; da aber auch umgekehrt jedem solchen Paare wegen

$$\mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{a}\mathfrak{b})$$

ein Ideal $\mathfrak{j} = \mathfrak{a}\mathfrak{b}$ entspricht, dessen Norm ab ist, so ist die Anzahl der letzteren Ideale gleich der Anzahl jener Paare, d. h. die Gleichung (66) bewiesen — Bildet man daher das Produkt aller, den sämtlichen rationalen Primzahlen p entsprechenden Ausdrücke (65), so wird seine Entwicklung zum allgemeinen Gliede den Ausdruck

$$\frac{F(\nu)}{\nu^\lambda}$$

haben, unter ν jede positive ganze Zahl verstanden, und die Formel (59^c) kehrt so in die frühere Gestalt (59^a) wieder zurück.

9. Erinnern wir uns ferner der Darstellung (33) sämtlicher Idealklassen aus gewissen fundamentalen. Ihr zufolge kann jede Klasse C durch die Wahl der Exponenten $x_1, x_2, \cdots, x_\sigma$ charakterisiert werden, die ihr in jener Darstellung zukommen. Führt man aber die σ Einheitswurzeln

$$e^{\frac{2\pi i}{h_1}}, \; e^{\frac{2\pi i}{h_2}}, \; \cdots, \; e^{\frac{2\pi i}{h_\sigma}}$$

ein, so sind mit jenen Exponenten auch die folgenden Potenzen derselben:

$$e^{\frac{2\pi i x_1}{h_1}}, \; e^{\frac{2\pi i x_2}{h_2}}, \; \cdots, \; e^{\frac{2\pi i x_\sigma}{h_\sigma}}, \tag{68}$$

sowie auch umgekehrt jene Exponenten mit diesen Einheitswurzeln zugleich bestimmt, und man darf daher auch diese Einheitswurzeln (68) als der Klasse C charakteristisch oder als ihren Charakter bezeichnen. Wir setzen demgemäß

$$\chi_1(C) = e^{\frac{2\pi i x_1}{h_1}}, \quad \chi_2(C) = e^{\frac{2\pi i x_2}{h_2}}, \quad \cdots, \quad \chi_\sigma(C) = e^{\frac{2\pi i x_\sigma}{h_\sigma}} \tag{69}$$

und nennen das System von Einzelcharakteren den Gesamtcharakter $\chi(C)$ der Klasse C. Da der Einzelcharakter $\chi_i(C)$, den Werten $1, 2, \cdots, h_i$ von x_i entsprechend h_i Werte hat, so beträgt die Anzahl der möglichen Gesamtcharaktere genau $h = h_1 h_2 \cdots h_\sigma$, d. h. soviel wie die Anzahl der Klassen. Bemerkt man nun, daß für jeden der Einzelcharaktere $\chi_i(C)$ seiner Definition zufolge sich die Gleichung

$$\chi_i(C'C'') = \chi_i(C') \cdot \chi_i(C'')$$

ergibt, so darf man auch für den Gesamtcharakter $\chi(C)$ die Beziehung

$$\chi(C'C'') = \chi(C') \cdot \chi(C'')$$

ansetzen. Den Charakter einer Klasse wollen wir aber auch als denjenigen eines jeden ihr zugehörigen Ideals $\mathfrak{j}$ auffassen; so ergibt sich dann aus der letzten Gleichung auch für irgend zwei Ideale des Körpers die folgende:

$$\chi(\mathfrak{j}'\mathfrak{j}'') = \chi(\mathfrak{j}') \cdot \chi(\mathfrak{j}''),$$

derzufolge die Formel

$$\sum_{\mathfrak{j}} \frac{\chi(\mathfrak{j})}{\mathfrak{N}(\mathfrak{j})^\lambda} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^\lambda}}, \tag{70}$$

in welcher auf der linken Seite die Summation auf sämtliche Ideale, zur Rechten aber die Multiplikation nur auf die Primideale des Körpers zu erstrecken ist, als richtig erkannt wird. Übrigens kann die Summe zur Linken auch folgendermaßen geschrieben werden:

$$\sum_{i=1}^{h}\left(\chi(C_i)\cdot\sum^{(i)}\frac{1}{\mathfrak{N}(\mathfrak{j})^{\lambda}}\right),$$

wenn die zweite der angedeuteten Summationen sich nur auf die Ideale der jedesmaligen Klasse C_i bezieht. Die Summe (70) ist das Analogon zu den Reihen, welche in der gewöhnlichen Zahlentheorie für die Verteilung der Primzahlen auf Linearformen von bestimmter Art oder auch auf die verschiedenen quadratischen Formen mit gegebener Determinante die Grundlage bilden (s. darüber „Analytische Zahlentheorie“ 4. und 10. Abschnitt), und wird für die entsprechenden Fragen der allgemeinen Idealtheorie von gleicher Bedeutung sein.

10. Wir wenden uns nunmehr von der Gesamtheit aller ganzen Zahlen des Körpers wieder zur Betrachtung irgend einer Ordnung $\mathfrak{o}$ solcher Zahlen. Die Äquivalenz zweier Ideale der Ordnung $\mathfrak{o}$ kann in ganz analoger Weise festgesetzt werden, wie diejenige der Körperideale, indem man zwei Ideale $\mathfrak{i}$, $\mathfrak{i}'$ in $\mathfrak{o}$ äquivalent nennt, wenn eine, offenbar dem Körper angehörige ganze oder gebrochene Zahl μ vorhanden ist, für welche

$$\mathfrak{i}' = \mu\cdot\mathfrak{i} \tag{71}$$

ist; wir setzen dabei aber auch hier die Norm von μ als positiv voraus. Hiernach leuchtet dann sogleich ein, daß Ideale der Ordnung $\mathfrak{o}$, welche ein- und demselben Ideale dieser Ordnung äquivalent sind, es auch unter einander sein müssen, und daß daher sämtliche Ideale der Ordnung in Klassen verteilt werden können von der Art, daß alle Ideale derselben Klasse unter einander äquivalent, zwei Ideale verschiedener Klassen aber nicht äquivalent sind. Daß die Anzahl dieser Klassen auch hier wieder eine nur endliche ist, könnte ähnlich bewiesen werden, wie für die Körperideale geschehen ist, wird sich aber durch die folgenden Untersuchungen ganz von selber ergeben. Da die Ordnung $\mathfrak{o}$ selbst

ein Ideal ist, so gibt es auch eine Klasse von Idealen in $\mathfrak{o}$, welche mit $\mathfrak{o}$ äquivalent sind; sie soll die Hauptklasse genannt werden und besteht nach der Definition nur aus Idealen in $\mathfrak{o}$ von der Form $\mathfrak{o}\mu$, worin μ eine Zahl des Körpers mit positiver Norm ist. Damit aber $\mathfrak{o}\mu$ ein Ideal in $\mathfrak{o}$ vorstelle, muß außerdem wegen $1 \succ \mathfrak{o}$ die Zahl μ selbst eine Zahl der Ordnung und nach Nr. 1

$$\mathfrak{o}\mu + \mathfrak{f} = \mathfrak{o}$$

sein. Diese für μ notwendigen Bedingungen genügen aber auch dazu, daß $\mathfrak{o}\mu$ ein Hauptideal in $\mathfrak{o}$ sei, da zugleich mit μ auch $\mathfrak{o}\mu$ in $\mathfrak{o}$ enthalten ist, nach den Definitionen dann $\mathfrak{o}\mu$ auch ein Ideal in $\mathfrak{o}$ und, da die Norm von μ positiv ist, mit $\mathfrak{o}$ äquivalent also ein Hauptideal sein wird.

Auch hier ist wieder der Satz von fundamentaler Bedeutung, daß zu jedem Ideale $\mathfrak{i}$ in $\mathfrak{o}$ ein zweites Ideal $\mathfrak{i}'$ in $\mathfrak{o}$ gefunden werden kann von der Beschaffenheit, daß das Produkt $\mathfrak{i} \cdot \mathfrak{i}'$ ein Hauptideal der Ordnung wird. Er ist auf Grund der in Nr. 2 gemachten Bemerkungen leicht zu beweisen. Wegen der Bedingung $\mathfrak{i} + \mathfrak{f} = \mathfrak{o}$ und da die Zahlen 0, 1 beide der Ordnung $\mathfrak{o}$ angehören, läßt sich nach Kap. 2, Nr. 3 eine Zahl μ bestimmen, welche den Kongruenzen

$$(72) \qquad \mu \equiv 0 \ (\text{mod. } \mathfrak{i}), \quad \mu \equiv 1 \ (\text{mod. } \mathfrak{f})$$

genügt, und diese dem Modulus $\mathfrak{i}$ angehörige Zahl kann zudem (nach Nr. 3) so gewählt werden, daß ihre Norm positiv wird. Da hiernach einerseits $\mu \succ \mathfrak{i} \succ \mathfrak{o}$ ist, folgt

$$\mathfrak{o}\mu \succ \mathfrak{o}\mathfrak{o} \text{ d. h. } \mathfrak{o}\mu \succ \mathfrak{o},$$

und da auch $\mathfrak{f} \succ \mathfrak{o}$ ist, ergibt sich

$$\mathfrak{o}\mu + \mathfrak{f} \succ \mathfrak{o}.$$

Andererseits ist nach der zweiten der Kongruenzen (72)

$$1 = \mu + \varphi,$$

wo φ eine Zahl des Ideals $\mathfrak{f}$ ist, also folgt

$$\mathfrak{o} \succ \mathfrak{o}\mu + \mathfrak{o}\mathfrak{f} \succ \mathfrak{o}\mu + \mathfrak{f}.$$

Durch Verbindung beider Resultate erschließt man die Gleichung

$$\mathfrak{o}\mu + \mathfrak{f} = \mathfrak{o}$$

und hieraus

$$\mathfrak{g}\mu + \mathfrak{f} = \mathfrak{g},$$

was zeigt, daß der wegen der ersten Kongruenz (72) in $\mathfrak{i}$ enthaltene Modul $\mathfrak{o}\mu$ ein Hauptideal der Ordnung ist. Nach Ende von Nr. 2 schließt man hiernach die Existenz eines Ideals $\mathfrak{i}'$ in $\mathfrak{o}$, für welches $\mathfrak{o}\mu = \mathfrak{i} \cdot \mathfrak{i}'$ ist, w. z. b. w.

Nach Nr. 1 ist das Produkt $\mathfrak{i}'\mathfrak{i}''$ zweier Ideale $\mathfrak{i}', \mathfrak{i}''$ in $\mathfrak{o}$ wieder ein Ideal in $\mathfrak{o}$; durchlaufen aber $\mathfrak{i}', \mathfrak{i}''$ alle Ideale zweier gegebenen Klassen C', C'', so werden ersichtlich die sämtlichen Produkte $\mathfrak{i}' \cdot \mathfrak{i}''$ unter einander äquivalent oder ein- und derselben dritten Klasse C angehörig sein, die wieder die aus C', C'' zusammengesetzte Klasse heißen und als das Produkt $C = C' \cdot C''$ geschrieben werden soll Offenbar ist die Ordnung der Faktoren eines solchen Produkts beliebig. Setzt man so eine Klasse C mit der Hauptklasse der Ordnung, welche H_0 heiße, zusammen, so entsteht wieder die Klasse C, in Zeichen:

$$C \cdot H_0 = C, \tag{73}$$

denn, sind $\mathfrak{i}$ und $\mathfrak{o}\mu$ Ideale in C und H_0 resp., so gehört das Produkt $\mathfrak{i} \cdot \mathfrak{o}\mu = \mathfrak{i}\mu$ derselben Klasse an wie $\mathfrak{i}$. Da ferner zu einem Ideale $\mathfrak{i}$ der Klasse C dem eben bewiesenen zufolge ein Ideal $\mathfrak{i}'$ einer gewissen Klasse C' gefunden werden kann, für welches $\mathfrak{i}\mathfrak{i}'$ ein Hauptideal also zu H_0 gehörig ist, so gibt es zu jeder Klasse C eine Klasse C' von der Beschaffenheit, daß die zusammengesetzte Klasse

$$C \cdot C' = H_0 \tag{74}$$

ist; es gibt auch nur eine solche Klasse, denn, wäre C'' noch eine andere derselben Art, sodaß auch $C \cdot C'' = H_0$ wäre, so ergäbe sich, wenn diese Gleichung mit C', die Gleichung (74) mit C'' zusammengesetzt würde, mit Rücksicht auf (73) die folgende:

$$CC'C'' = H_0 C' = H_0 C'' = C' = C''.$$

Die so eindeutig bestimmte Klasse C' wird die zur Klasse C reziproke oder inverse oder entgegengesetzte Klasse genannt, und es ist klar, daß umgekehrt C die zu C' entgegengesetzte Klasse ist. Aus einer Gleichheit zwischen Klassen von der Form

$$AC = BC$$

ergibt sich demnach immer die Gleichheit von A, B, da jene durch Zusammensetzung mit C' in die folgende:

$$A \cdot CC' = B \cdot CC',$$

d. h. $AH_0 = BH_0$ oder $A = B$ übergeht. Sind endlich A, B irgend zwei Idealklassen in $\mathfrak{o}$, so gibt es stets eine ganz bestimmte Klasse C in $\mathfrak{o}$ von der Art, daß

$$A = BC$$

ist; denn dieser Beziehung genügt die Klasse $C = AB'$, wo B' die zu B entgegengesetzte Klasse bedeutet, und offenbar die so bestimmte Klasse allein.

11. Die Anzahl der Idealklassen einer beliebigen Ordnung $\mathfrak{o}$ kann auf ganz entsprechende Weise bestimmt werden, wie diejenige der Idealklassen der Gesamtheit $\mathfrak{g}$ und läßt dann eine Vergleichung mit der letzteren zu, die in einer sehr eleganten Formel ihren Ausdruck findet. Bei der Übereinstimmung der hier erforderlichen Betrachtungen mit den Entwicklungen der Nr. 6 und 7 dürfen wir uns kurz fassen, indem wir nur die Hauptmomente derselben hervorheben.

Wie in Nr. 6 beginnen wir mit der Aufsuchung des Grenzwertes

$$\lim_{t=\infty} \cdot \left(\frac{T}{t}\right),$$

worin T die Anzahl der Hauptideale $\mathfrak{o}\alpha$ in $\mathfrak{o}$ bedeutet, deren Normen nicht größer als t und welche durch ein gegebenes Ideal $\mathfrak{i}$ in $\mathfrak{o}$ teilbar sind. Diese Hauptideale $\mathfrak{o}\alpha$ sind dadurch charakterisiert, daß

1) α eine dem Ideale $\mathfrak{i}$ angehörige Zahl, also, wenn $\alpha_1, \alpha_2, \cdots, \alpha_n$ die Basiszahlen des Ideals bedeuten, von der Form

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

mit ganzzahligen Koeffizienten a_i ist,

2) daß $\mathfrak{o}\alpha + \mathfrak{f} = \mathfrak{o}$ ist, und

3) daß $0 < N(\alpha) \overline{\gtrless} t$ ist.

Die beiden ersten dieser Bedingungen sprechen sich in den Kongruenzen aus:

$$(75) \qquad \alpha \equiv 0 \pmod{\mathfrak{i}}, \quad \alpha \equiv \omega \pmod{\mathfrak{f}},$$

wo ω irgend eine der (mod. $\mathfrak{f}$) inkongruenten Zahlen der Ord-

nung $\mathfrak{o}$ bezeichnet, für welche $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ ist; die Anzahl der letzteren Zahlen heiße $\varphi_0(\mathfrak{f})$. Da wegen der Bedingung $\mathfrak{i} + \mathfrak{f} = \mathfrak{o}$ nach Kap. 2, Nr. 3 die Kongruenzen (75) für jede solche Zahl ω miteinander verträglich sind und ihre Lösungen eine bestimmte Klasse kongruenter Zahlen (mod. $\mathfrak{i} - \mathfrak{f}$) ausmachen, so gibt es $\varphi_0(\mathfrak{f})$ nach dem Modulus $\mathfrak{i} - \mathfrak{f}$ inkongruente Zahlen α, welche den obigen Bedingungen 1) und 2) genügen, oder sämtliche ihnen genügende Zahlen α zerfallen in $\varphi_0(\mathfrak{f})$ Zahlenklassen (mod. $\mathfrak{i} - \mathfrak{f}$). Man sieht zunächst leicht ein, daß

$$\mathfrak{i} - \mathfrak{f} = \mathfrak{i}\mathfrak{f}$$

ist. Denn einerseits folgt aus $\mathfrak{f} \succ \mathfrak{o}$ und $\mathfrak{i} \succ \mathfrak{o} \succ \mathfrak{g}$, daß $\mathfrak{i}\mathfrak{f}$ sowohl in $\mathfrak{o}\mathfrak{i} = \mathfrak{i}$ als in $\mathfrak{f}\mathfrak{g} = \mathfrak{f}$, mithin in $\mathfrak{i} - \mathfrak{f}$ enthalten ist; andererseits ist $\mathfrak{i} - \mathfrak{f}$, weil in $\mathfrak{i}$, auch in $\mathfrak{g}\mathfrak{i}$, und weil auch in dem zu $\mathfrak{g}\mathfrak{i}$ relativ primen Ideale $\mathfrak{f}$ enthalten, auch in ihrem kleinsten gemeinsamen Vielfachen d. i. ihrem Produkte

$$\mathfrak{g}\mathfrak{i} \cdot \mathfrak{f} = \mathfrak{i}\mathfrak{f}$$

enthalten. — Ferner ist aber nach dem Schlusse des 4. Kapitels, wenn

$$k = (\mathfrak{g}, \mathfrak{o}) = \mathfrak{N}(\mathfrak{o})$$

gesetzt wird, das Hauptideal $\mathfrak{g}k$ in $\mathfrak{f}$ enthalten. Daraus folgt

$$\mathfrak{i} \cdot k \succ \mathfrak{i} \cdot \mathfrak{f}$$

und demnach setzt sich jede der gedachten $\varphi_0(\mathfrak{f})$ Zahlenklassen (mod. $\mathfrak{i}\mathfrak{f}$) aus einer Anzahl $(\mathfrak{i}\mathfrak{f}, \mathfrak{i}k)$ engerer Zahlenklassen zusammen, sodaß die Anzahl inkongruenter Klassen, in welche die oben gedachten Zahlen α (mod. $\mathfrak{i}k$), d. i. in bezug auf den Modulus

$$[k\alpha_1, k\alpha_2, \cdots, k\alpha_n] \tag{76}$$

zerfallen,

$$c = \varphi_0(\mathfrak{f}) \cdot (\mathfrak{i}\mathfrak{f}, \mathfrak{i}k) \tag{77}$$

beträgt.

Es ist wesentlich zu beweisen, daß diese Zahl c eine, von dem besonderen Ideale $\mathfrak{i}$, das gerade betrachtet wird, unabhängige Konstante ist. Hierzu bemerke man, daß aus

$$\mathfrak{i} \succ \mathfrak{o} \succ \mathfrak{g}, \quad \mathfrak{i} \succ \mathfrak{g}\mathfrak{i} \succ \mathfrak{g}$$

die Gleichungen

$$(\mathfrak{g}, \mathfrak{i}) = (\mathfrak{g}, \mathfrak{o}) \cdot (\mathfrak{o}, \mathfrak{i}), \quad (\mathfrak{g}, \mathfrak{i}) = (\mathfrak{g}, \mathfrak{g}\mathfrak{i}) \cdot (\mathfrak{g}\mathfrak{i}, \mathfrak{i}),$$

folglich diese andere:

$$(\mathfrak{g}, \mathfrak{o}) \cdot (\mathfrak{o}, \mathfrak{i}) = (\mathfrak{g}, \mathfrak{g}\mathfrak{i}) \cdot (\mathfrak{g}\mathfrak{i}, \mathfrak{i}),$$

d. h., da $\mathfrak{N}'(\mathfrak{i}) = (\mathfrak{o}, \mathfrak{i}) = \mathfrak{N}(\mathfrak{g}\mathfrak{i}) = (\mathfrak{g}, \mathfrak{g}\mathfrak{i})$ ist, die Gleichung

$$k = (\mathfrak{g}\mathfrak{i}, \mathfrak{i})$$

zu erschließen ist, der offenbar auch die Form

$$k = (k\mathfrak{g}\mathfrak{i}, k\mathfrak{i}) \tag{78}$$

gegeben werden kann. Andererseits bestehen die Ungleichheiten

$$k\mathfrak{g}\mathfrak{i} \succ \mathfrak{i}\mathfrak{g}\mathfrak{f} = \mathfrak{i}\mathfrak{f} \succ \mathfrak{g},$$

folglich ist

$$(\mathfrak{g}, k\mathfrak{g}\mathfrak{i}) = (\mathfrak{g}, \mathfrak{f}\mathfrak{i}) \cdot (\mathfrak{f}\mathfrak{i}, \mathfrak{g}k\mathfrak{i}),$$

also

$$(\mathfrak{f}\mathfrak{i}, \mathfrak{g}k\mathfrak{i}) = \frac{\mathfrak{N}(\mathfrak{g}k \cdot \mathfrak{i})}{\mathfrak{N}(\mathfrak{f} \cdot \mathfrak{i})} = \frac{\mathfrak{N}(\mathfrak{g}k \cdot \mathfrak{g}\mathfrak{i})}{\mathfrak{N}(\mathfrak{f} \cdot \mathfrak{g}\mathfrak{i})} = \frac{\mathfrak{N}(\mathfrak{g}k)}{\mathfrak{N}(\mathfrak{f})} = \frac{k^n}{\mathfrak{N}(\mathfrak{f})}.$$

Die Verbindung dieser Formel mit der Formel (78) ergibt

$$(\mathfrak{f}\mathfrak{i}, k\mathfrak{i}) = (\mathfrak{f}\mathfrak{i}, \mathfrak{g}k\mathfrak{i}) \cdot (\mathfrak{g}k\mathfrak{i}, k\mathfrak{i}) = \frac{k^{n+1}}{\mathfrak{N}(\mathfrak{f})}$$

und folglich nach (77)

$$c = \frac{\varphi_0(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot k^{n+1}, \tag{79}$$

d. i. ein nur von der Ordnung $\mathfrak{o}$ bestimmter Wert.

Denkt man sich nun aus jeder der c Klassen (mod. $k\mathfrak{i}$) je eine Zahl

$$c_1^{(i)}\alpha_1 + c_2^{(i)}\alpha_2 + \cdots + c_n^{(i)}\alpha_n$$
$$(i = 1, 2, \cdots, c)$$

ausgewählt, so werden sämtliche Zahlen α, welche die beiden obigen Bedingungen 1) und 2) erfüllen, gegeben durch die c Ausdrücke

$$\alpha = (c_1^{(i)} + ka_1)\alpha_1 + (c_2^{(i)} + ka_2)\alpha_2 + \cdots + (c_n^{(i)} + ka_n)\alpha_n, \tag{80}$$
$$(i = 1, 2, \cdots, c)$$

wenn darin die a_i sämtliche rationale ganze Zahlen durchlaufen, und offenbar jede von ihnen auch nur einmal. Von all' diesen Zahlen α sind jedoch wegen 3) nur diejenigen beizubehalten, deren Norm positiv und nicht größer als t ist, in Zeichen:

$$0 < N(\alpha) \overline{\gtrless} t. \tag{81}$$

Wenn nun zwar hiermit auch die sämtlichen durch $\mathfrak{i}$ teilbaren Hauptideale $\mathfrak{o}\alpha$, um welche es sich handelt, bestimmt

sind, so ist doch zu bemerken, daß man jedes derselben unendlich oft erhält, da, wenn α_0 irgend eine der angegebenen Zahlen und ε eine Einheit der Ordnung mit positiver Norm bezeichnet, offenbar auch $\varepsilon\alpha_0$ eine jener Zahlen darstellt, die unendlich vielen Hauptideale $\mathfrak{o}\varepsilon\alpha_0$ aber, übrigens auch nur diese, dem Hauptideale $\mathfrak{o}\alpha_0$ gleich sein werden. Wählt man indessen irgend ein System von $s-1$ unabhängigen Einheiten in $\mathfrak{o}$, wie in Nr. 9 des vorigen Kapitels, z. B. ein System von Fundamentaleinheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$, so lassen sich von den sämtlichen zu α_0 eigentlich assoziierten Zahlen $\alpha = \varepsilon\alpha_0$ durch die Bedingung, daß für die zugehörigen Exponenten $e_i(\alpha)$ in den Gleichungen

$$e_1(\alpha)l_{i1} + e_2(\alpha)l_{i2} + \cdots + e_{s-1}(\alpha)l_{i,s-1} + f\cdot c_i = l_i(\alpha)\,. \qquad (i = 1, 2, \cdots, s) \tag{82}$$

die Ungleichheiten

$$0 \gtreqless e_i(\alpha) < 1 \qquad (i = 1, 2, \cdots, s-1) \tag{83}$$

erfüllt seien, genau soviel isolieren, als die Anzahl der bezüglichen reduzierten Einheiten oder der in der Ordnung vorhandenen Einheitswurzeln beträgt, die wir ϱ_0 nennen wollen. Demnach beträgt die Anzahl derjenigen Zahlen α, welche durch die Formeln (80) bestimmt sind und den Ungleichheiten (81) und (83) genügen, offenbar $\varrho_0 \cdot T$.

Verfährt man nun weiter ganz wie in Nr. 6, so findet sich der Grenzwert von $\frac{T}{t}$ wieder durch ein n-faches Integral bestimmt, bei welchem jedoch die Zuordnung der Variabeln u_i zu den Koeffizienten der Zahlen α in zwei Punkten von der früheren sich unterscheidet. Zunächst sind dort die Zahlen α auf die einzige Linearform (37) beschränkt, während ihnen hier die c verschiedenen Linearformen (80) verstattet sind. Aber, wenn man zunächst auch nur diejenigen α in Betracht zieht, welche einer einzigen dieser Linearformen entsprechen, so werden die Variabeln u_i doch, statt durch die dortigen Formeln (48) bestimmt zu werden, mit den Zahlen α jetzt durch die Formeln

$$u_1 = \delta c_1^{(i)} + \delta k a_1,\ u_2 = \delta c_2^{(i)} + \delta k a_2,\ \cdots,\ u_n = \delta c_n^{(i)} + \delta k a_n$$

verbunden sein. Bei unendlich wachsendem Werte von t oder

unendlicher Abnahme von $\delta = \frac{1}{t^{1/n}}$ gehen diese Formeln in die anderen:

$$u_1 = \delta \cdot ka_1,\ u_2 = \delta \cdot ka_2,\ \cdots,\ u_n = \delta \cdot ka_n$$

über, was zur Folge hat, daß die Formel (49) die Gestalt annimmt

$$(84)\qquad \int du_1 \cdot du_2 \cdots du_n = \varrho_0 \cdot k^n \cdot \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) \cdot$$

Hier ergibt sich aber nun, wenn man noch bedenkt, daß die Diskriminante $\varDelta(\alpha_1, \alpha_2, \cdots, \alpha_n)$ des Ideales $\mathfrak{i}$ gleich $\mathfrak{N}'(\mathfrak{i})^2 \cdot D$ ist, unter D die Diskriminante der Ordnung $\mathfrak{o}$ verstanden, der Wert des auf **eine** jener Linearformen (80) beschränkten Integrales analog mit Nr. 6 gleich

$$\frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot |\, l_k(\varepsilon_i) \,|}{\mathfrak{N}'(\mathfrak{i}) \cdot \sqrt{(D)}},$$

ein Wert, der nichts an sich enthält, was der besonderen eben betrachteten Linearform (80) charakteristisch wäre, und daher für jede derselben Geltung hat; also folgt für das gesamte, alle c Linearformen umfassende Integral (84) der c-fache Wert und folglich bei Beachtung von (79) und, weil

$$D = \mathfrak{N}(\mathfrak{o})^2 \cdot \mathrm{D} = k^2 \cdot \mathrm{D}$$

ist, **nachstehende Formel:**

$$(85)\qquad \lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \frac{\varphi_0(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{s-\sigma} \cdot \pi^{n-s} \cdot Q_0}{\mathfrak{N}'(\mathfrak{i}) \sqrt{(\mathrm{D})}},$$

wenn zur Abkürzung

$$(86)\qquad Q_0 = \frac{|\, l_k(\varepsilon_i) \,|}{\varrho_0}$$

den Quotienten zwischen dem Regulator des Systems von Fundamentaleinheiten und der Anzahl der Einheitswurzeln der Ordnung $\mathfrak{o}$ bezeichnet.

12. Die Formel (85) läßt sich anders schreiben, wenn man bemerkt, daß

$$\lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \lim_{\nu=\infty} \cdot \frac{F(1) + F(2) + \cdots + F(\nu)}{\nu}$$

gesetzt werden darf, unter $F(\nu)$ die Anzahl derjenigen durch $\mathfrak{i}$

teilbaren Hauptideale in $\mathfrak{o}$ verstanden, deren Normen gleich ν sind. Ganz analog wie in Nr. 7 ist dann nämlich einzusehen, daß

$$\lim_{t=\infty} \cdot \left(\frac{T}{t}\right) = \lim_{\lambda=1} \cdot (\lambda - 1) \sum \frac{1}{\mathfrak{N}'(\mathfrak{o}\alpha)^{\lambda}}$$

ist, wo die Summation sich auf alle durch $\mathfrak{i}$ teilbaren Hauptideale in $\mathfrak{o}$ erstreckt. Demgemäß nimmt die Formel (85) die Gestalt an:

$$\lim_{\lambda=1} \cdot (\lambda - 1) \sum \frac{1}{\mathfrak{N}'(\mathfrak{o}\alpha)^{\lambda}} = \frac{\varphi_0(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{s-\sigma}\pi^{n-s} Q_0}{\mathfrak{N}'(\mathfrak{i})\sqrt{(D)}}. \tag{87}$$

Durchläuft nun $\mathfrak{a}$ alle Ideale einer gegebenen Klasse C in $\mathfrak{o}$ und bezeichnet $\mathfrak{i}$ ein bestimmtes Ideal der entgegengesetzten Klasse C', so ist jedes Produkt $\mathfrak{a}\mathfrak{i}$ ein Ideal in $\mathfrak{o}$, welches notwendig zur Hauptklasse $H_0 = CC'$ gehört, also ein durch $\mathfrak{i}$ teilbares Hauptideal in $\mathfrak{o}$ ist; zudem bilden aber alle diese Produkte auch die Gesamtheit der Hauptideale dieser Art, denn, ist $\mathfrak{o}\alpha$ ein durch $\mathfrak{i}$ teilbares Hauptideal, so gibt es ein ganz bestimmtes Ideal $\mathfrak{a}$ in $\mathfrak{o}$ von der Art, daß $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{i}$ ist, welches daher der zur Klasse C', in welcher $\mathfrak{i}$ liegt, entgegengesetzten Klasse C angehören muß. Hiernach wird, weil

$$\mathfrak{N}'(\mathfrak{a}\mathfrak{i}) = \mathfrak{N}'(\mathfrak{a}) \cdot \mathfrak{N}'(\mathfrak{i})$$

ist, die über all' die gedachten Hauptideale erstreckte Summe

$$\sum \frac{1}{\mathfrak{N}'(\mathfrak{o}\alpha)^{\lambda}} = \frac{1}{\mathfrak{N}'(\mathfrak{i})^{\lambda}} \cdot \sum \frac{1}{\mathfrak{N}'(\mathfrak{a})^{\lambda}},$$

wo die Summe zur Rechten alle Ideale der Klasse C umfaßt Wegen (87) erhält man daher die neue Gleichung

$$\lim_{\lambda=1} \cdot (\lambda - 1) \sum \frac{1}{\mathfrak{N}'(\mathfrak{a})^{\lambda}} = \frac{\varphi_0(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{s-\sigma}\pi^{n-s} Q_0}{\sqrt{(D)}}. \tag{88}$$

Man erkennt aus derselben, daß die links stehende Summe den gleichen Wert hat für jede der Klassen äquivalenter Ideale in $\mathfrak{o}$, auf welche man die Summation beziehen mag.

Nunmehr bezeichne $\mathfrak{i}$ jedes Ideal in $\mathfrak{o}$ und $Z_0(\lambda)$ für $\lambda > 1$ die auf alle diese bezogene Summe

$$Z_0(\lambda) = \sum \frac{1}{\mathfrak{N}'(\mathfrak{i})^{\lambda}}; \tag{89}$$

wir setzen ferner, wie in Nr. 7,

$$Z(\lambda) = \sum \frac{1}{\mathfrak{N}(\mathfrak{j})^\lambda}, \tag{90}$$

indem wir die angedeutete Summation auf alle Ideale $\mathfrak{j}$ des Körpers beziehen. Hierfür kann nach (59^b) geschrieben werden:

$$Z(\lambda) = \prod_{\mathfrak{p}} \left(\frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^\lambda}} \right)$$

oder, wenn $\mathfrak{p}'$ die in $\mathfrak{f}$ aufgehenden, $\mathfrak{p}''$ alle übrigen Primideale in $\mathfrak{g}$ bezeichnet

$$Z(\lambda) = \prod_{\mathfrak{p}'} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p}')^\lambda}} \cdot \prod_{\mathfrak{p}''} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p}'')^\lambda}}$$

d. i.

$$Z(\lambda) = \prod_{\mathfrak{p}'} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p}')^\lambda}} \cdot \sum{}' \frac{1}{\mathfrak{N}(\mathfrak{j})^\lambda}, \tag{91}$$

wenn nun die letztere Summation nur auf diejenigen Ideale $\mathfrak{j}$ in $\mathfrak{g}$ erstreckt wird, welche prim sind zu $\mathfrak{f}$. Nach Nr. 2 entsprechen sich aber immer ein Ideal $\mathfrak{i}$ in $\mathfrak{o}$ und ein zu $\mathfrak{f}$ primes Ideal $\mathfrak{j}$ in $\mathfrak{g}$ in der Weise, daß $\mathfrak{j} = \mathfrak{g}\mathfrak{i}$ und $\mathfrak{N}(\mathfrak{j}) = \mathfrak{N}'(\mathfrak{i})$ wird. Demnach ist die vorgedachte Summe nichts anderes als $Z_0(\lambda)$, und da nach (116) des 6. Kapitels

$$\prod_{\mathfrak{p}'} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p}')}\right) = \frac{\varphi(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})}$$

gesetzt werden kann, so ergibt sich aus (91) nachstehende Beziehung:

$$\frac{\varphi(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \lim_{\lambda=1} \cdot (\lambda - 1)\, Z(\lambda) = \lim_{\lambda=1} \cdot (\lambda - 1)\, Z_0(\lambda),$$

oder mit Beachtung von (62) und (64) diese andere:

$$\frac{\varphi(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{r-\sigma}\pi^{n-s} Q}{\sqrt{(D)}} \cdot h = \lim_{\lambda=1} \cdot (\lambda - 1)\, Z_0(\lambda).$$

Ihr zufolge ist der Ausdruck zur Rechten ein endlicher Wert. Da derselbe sich nun aus den verschiedenen Teilen (88), welche den einzelnen Klassen äquivalenter Ideale in $\mathfrak{o}$ entsprechen, durch Addition zusammensetzt, jeder dieser Teile aber den

gleichen Wert hat, so kann auch die Anzahl dieser Teile d. i. die Klassenanzahl h_0 für die Ideale in $\mathfrak{o}$ nur eine endliche sein, und durch Substitution des Wertes (88) findet sich daher aus der vorigen Gleichung die folgende:

$$\frac{\varphi(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{s-\sigma}\pi^{n-\sigma}Q}{\sqrt{(D)}} \cdot h = \frac{\varphi_0(\mathfrak{f})}{\mathfrak{N}(\mathfrak{f})} \cdot \frac{2^{s-\sigma}\pi^{n-s}Q_0}{\sqrt{(D)}} \cdot h_0$$

oder einfacher diese andere:

$$\frac{h}{h_0} = \frac{\varphi_0(\mathfrak{f})}{\varphi(\mathfrak{f})} \cdot \frac{Q_0}{Q}. \tag{92}$$

Hierdurch ist das Verhältnis der Anzahl der Klassen äquivalenter Ideale in $\mathfrak{g}$ zu derjenigen in einer beliebigen Ordnung $\mathfrak{o}$, und folglich auch das Verhältnis dieser Anzahlen für irgend zwei Ordnungen nach der analytischen Methode von *Dirichlet* bestimmt.

13. Die für diesen Zweck angestellten Betrachtungen entsprechen genau denjenigen, durch welche einst Dirichlet die analoge Aufgabe für die quadratischen Zahlenkörper behandelt oder, was auf dasselbe hinauskommt, das Verhältnis zwischen der Anzahl nicht äquivalenter Klassen für verschiedene Ordnungen quadratischer Formen einer gegebenen Determinante bestimmt hat. Doch hatte schon vorher Gauß dieselbe Aufgabe ohne die Hilfsmittel der Analysis gelöst, und die Art seiner Lösung zeichnete sich vorteilhaft dadurch aus, daß sie einerseits der Bestimmung der Klassenanzahlen selbst, wie sie wenigstens bis zu einem gewissen Grade bei der Dirichletschen Methode nötig ist, gar nicht bedarf, um die Vergleichung für die verschiedenen Ordnungen zu ermöglichen, andererseits aber tiefer aus dem Zusammenhange der verschiedenen Ordnungen unter einander geschöpft ist. Aus diesen Gründen ist es angemessen, auch für das allgemeinere Problem hier noch die Gaußische Methode im Anschluß an Dedekind zur Verwendung zu bringen.

Da jedem Ideale $\mathfrak{i}$ in $\mathfrak{o}$ ein Ideal $\mathfrak{j}$ in $\mathfrak{g}$ entspricht, das mit jenem durch die Gleichung $\mathfrak{j} = \mathfrak{g}\mathfrak{i}$ verknüpft ist, so folgt offenbar für die Klassen H, C, C_0, denen resp. die Ideale $\mathfrak{g}$, $\mathfrak{j}$, $\mathfrak{i}$ angehören, die Beziehung $C = H \cdot C_0$; demnach bringt

erstens jede Idealklasse in $\mathfrak{o}$ durch Zusammensetzung mit der Hauptklasse H eine bestimmte Idealklasse C in $\mathfrak{g}$ hervor. So ist wegen $\mathfrak{g}\mathfrak{o} = \mathfrak{g}$ insbesondere

(93) $$H \cdot H_0 = H.$$

Es ist jedoch denkbar, daß mehrere Idealklassen in $\mathfrak{o}$ auf solche Weise dieselbe Idealklasse C in $\mathfrak{g}$ hervorbringen. Sei also K_0 eine zweite Klasse derselben Beschaffenheit, sodaß auch $C = H \cdot K_0$ gesetzt werden kann. Dann folgt

$$H \cdot K_0 = H \cdot C_0$$

also, wenn C_0' die zu C_0 entgegengesetzte Klasse bezeichnet, mithin $C_0 C_0' = H_0$ ist,

$$HK_0C_0' = HC_0C_0' = HH_0 = H.$$

Setzt man also

$$K_0 C_0' = M_0 \quad \text{oder} \quad K_0 = M_0 C_0,$$

so leistet M_0 der Gleichung

(94) $$H \cdot M_0 = H$$

Genüge; und umgekehrt wird, wenn M_0 eine dieser Gleichung genügende Klasse in $\mathfrak{o}$ ist, für jede Klasse $K_0 = M_0 C_0$ die Beziehung $C = H \cdot K_0$ erfüllt sein. Man darf mithin *zweitens* sagen: Entsteht C aus C_0 durch Zusammensetzung mit der Hauptklasse H, so entsteht es so gleichfalls und ausschließlich aus allen Klassen des Komplexes

(95) $$M_0 \cdot C_0,$$

in welchem M_0 jede der Gleichung (94) genügende Idealklasse in $\mathfrak{o}$ bedeutet. Zudem sind die den verschiedenen Lösungen M_0 dieser Gleichung entsprechenden Glieder des Komplexes nach Ende von Nr. 10 voneinander verschieden. Wir werden in der Folge beweisen, daß die Anzahl dieser Klassen M_0 nur eine endliche ist, und nennen sie m. Daher werden immer je m Idealklassen in $\mathfrak{o}$, welche einem solchen Komplexe von der Form (95) angehören, und nur diese, durch Zusammensetzung mit der Hauptklasse H in $\mathfrak{g}$ eine bestimmte Idealklasse in $\mathfrak{g}$ hervorbringen.

Nun lassen sich aber sämtliche Idealklassen in $\mathfrak{o}$ in eine endliche Anzahl Komplexe von der Form (95) verteilen. Die Idealklassen M_0 bilden nämlich eine Gruppe von Klassen, die wir die Gruppe (M_0) nennen, indem das Produkt von irgend zwei von ihnen sets wieder eine von ihnen ist. In der Tat, wenn $\mathfrak{M}_0$, $\mathfrak{N}_0$ zwei solche Klassen sind, also

$$H \cdot \mathfrak{M}_0 = H, \; H\mathfrak{N}_0 = H$$

ist, so ist auch

$$H \cdot \mathfrak{M}_0\mathfrak{N}_0 = H \cdot \mathfrak{N}_0 = H.$$

Zu der Gruppe gehört insbesondere offenbar auch die Hauptklasse H_0 in $\mathfrak{o}$; ist ferner $\mathfrak{M}_0$ eine Klasse der Gruppe (M_0), so gehört ihr auch die entgegengesetzte Klasse $\mathfrak{M}_0'$ an, da aus

$$H \cdot \mathfrak{M}_0 = H$$

auch

$$H \cdot \mathfrak{M}_0' = H \cdot \mathfrak{M}_0\mathfrak{M}_0' = HH_0 = H$$

folgt. Auf Grund dieser Bemerkungen erkennt man leicht, daß, wenn eine Idealklasse K_0 in $\mathfrak{o}$ dem Komplexe (95) nicht angehört, auch der gesamte ihr entsprechende Komplex M_0K_0 von jenem verschieden sein muß. Denn, wären etwa die diesen beiden Komplexen resp. angehörigen Klassen

$$\mathfrak{M}_0C_0, \; \mathfrak{N}_0K_0,$$

wo $\mathfrak{M}_0$, $\mathfrak{N}_0$ bestimmte Klassen der Gruppe (M_0) bedeuten, einander gleich, so ergäbe sich

$$K_0 = H_0K_0 = \mathfrak{N}_0\mathfrak{N}_0'K_0 = \mathfrak{M}_0\mathfrak{N}_0'C_0$$

und somit wäre K_0, da das Produkt der beiden zur Gruppe (M_0) gehörigen Klassen $\mathfrak{M}_0$, $\mathfrak{N}_0'$ ihr ebenfalls angehört, gegen die Voraussetzung ein Glied des Komplexes (95).

Hieraus folgt nun offenbar, daß, wie behauptet, alle Idealklassen in $\mathfrak{o}$ sich in eine Anzahl Komplexe von je m verschiedenen Klassen verteilen lassen, eine Anzahl, welche nur endlich sein kann, nämlich nicht größer als die Anzahl h der Idealklassen in $\mathfrak{g}$, da jedem solchen Komplexe eine bestimmte dieser Idealklassen und verschiedenen Komplexen auch verschiedene der letzteren entsprechen, indem sie durch jene mittels Zusammensetzung mit H hervorgebracht

werden. Die Anzahl der Komplexe von der Form (95) kann aber auch nicht kleiner sein als h und ist demnach gleich h. Denn es gilt auch der zum ersten Punkte umgekehrte Satz: Jede Idealklasse C in $\mathfrak{g}$ wird aus einer Idealklasse in $\mathfrak{o}$ durch Zusammensetzung mit H hervorgebracht und entspricht somit einem der Komplexe von der Form (95). In der Tat gibt es nach Nr. 3 in C ein Ideal $\mathfrak{j}$, welches zu einem beliebig gegebenen Ideale, als welches wir hier das Ideal $\mathfrak{f}$ wählen, relativ prim ist; alsdann ist aber nach Nr. 2 das kleinste gemeinsame Vielfache $\mathfrak{i} = \mathfrak{j} - \mathfrak{o}$ von $\mathfrak{j}$ und $\mathfrak{o}$ ein Ideal in $\mathfrak{o}$, für welches $\mathfrak{j} = \mathfrak{g}\mathfrak{i}$ ist, und demnach leistet die Klasse C_0, welcher $\mathfrak{i}$ angehört, der Bedingung $C = H \cdot C_0$ Genüge.

Aus diesen Umständen ist zu schließen, daß die gesamte Menge aller Idealklassen in $\mathfrak{o}$ sich in h Komplexe von der Form (95) von je m Klassen verteilen läßt, und daß demgemäß auch die Anzahl h_0 der Idealklassen der Ordnung $\mathfrak{o}$ nur eine endliche und durch die Formel

$$h_0 = m \cdot h \tag{96}$$

bestimmt ist.

14. Es erübrigt nur der Nachweis, daß m eine endliche Zahl ist. Wir führen denselben, indem wir diese Zahl wirklich bestimmen.

Hierzu gibt folgende Erwägung die wesentliche Grundlage. Ist M_0 eine Idealklasse in $\mathfrak{o}$, welche der Gleichung (94) genügt und $\mathfrak{i}$ irgend ein darin enthaltenes Ideal, so muß das Produkt $\mathfrak{g}\mathfrak{i}$, welches ein zu $\mathfrak{f}$ primes Ideal in $\mathfrak{g}$ ist, wegen (94) notwendig der Hauptklasse H angehören, d. h. ein Hauptideal $\mathfrak{g}\alpha$ sein, wo α eine zu $\mathfrak{f}$ prime Zahl in $\mathfrak{g}$ mit positiver Norm bedeutet. Umgekehrt entspricht aber auch jeder solchen Zahl α oder dem ihm zugehörigen zu $\mathfrak{f}$ primen Hauptideale $\mathfrak{g}\alpha$ nach Nr. 2 ein bestimmtes Ideal $\mathfrak{i}$ in $\mathfrak{o}$, für welches $\mathfrak{g}\mathfrak{i} = \mathfrak{g}\alpha$ ist, und welches daher einer bestimmten der Idealklassen M_0 angehört, die der Gleichung (94) genügen. So ist also jeder der gedachten Zahlen α eine und nur eine einzige Klasse aus der Gruppe (M_0) zugeordnet. Dagegen ist es denkbar, daß

mehreren jener Zahlen α ein- und dieselbe Klasse M_0 zugeordnet ist. In dieser Hinsicht gilt der folgende Satz:

Sind α, α_1 zwei Zahlen in $\mathfrak{g}$ mit positiver Norm und zu $\mathfrak{f}$ relativ prim, so entspricht ihnen dann und nur dann dieselbe Klasse M_0, wenn die Kongruenz

$$(97) \qquad \alpha_1 \equiv \alpha \varepsilon \omega \pmod{\mathfrak{f}}$$

erfüllt ist, worin ε eine Einheit und ω eine der Bedingung $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ genügende Zahl der Ordnung $\mathfrak{o}$, beide mit positiver Norm, bedeuten.

Zum Beweise bemerke man zuvörderst: wenn $\mathfrak{i}$ das dem Ideale $\mathfrak{g}\alpha$ entsprechende Ideal in M_0 bezeichnet, sodaß $\mathfrak{g}\mathfrak{i} = \mathfrak{g}\alpha$ ist, so gibt es wegen $\mathfrak{i} + \mathfrak{f} = \mathfrak{o}$ eine Zahl β der Ordnung $\mathfrak{o}$, welche den Kongruenzen

$$(98) \qquad \beta \equiv 0 \pmod{\mathfrak{i}}, \quad \beta \equiv 1 \pmod{\mathfrak{f}}$$

genügt und deren Norm nach dem allgemeinen Satze in Nr. 3 positiv gedacht werden darf; für sie ist (s. den Beweis des fundamentalen Satzes in Nr. 10) $\mathfrak{o}\beta$ ein durch $\mathfrak{i}$ teilbares Hauptideal in $\mathfrak{o}$. Setzt man also

$$(99) \qquad \mathfrak{o}\beta = \mathfrak{i} \cdot \mathfrak{i}',$$

so ist $\mathfrak{i}'$ ein Ideal in $\mathfrak{o}$, welches zu der zu M_0 entgegengesetzten Klasse M_0' gehören muß. Da ferner aus (99) die Gleichung

$$\mathfrak{g}\beta = \mathfrak{g}\mathfrak{i} \cdot \mathfrak{i}' = \mathfrak{g}\mathfrak{i}' \cdot \alpha$$

hervorgeht, so ist notwendig β ein Vielfaches von α,

$$(100) \qquad \beta = \alpha\gamma,$$

wo γ eine ganze Zahl ist, deren Norm, wie diejenigen von α und β, positiv ist; auch ist γ relativ prim zu $\mathfrak{f}$, da nach der zweiten der Kongruenzen (98) $\alpha\gamma \equiv 1 \pmod{\mathfrak{f}}$ ist. Wegen (100) ist ferner $\mathfrak{g}\alpha\gamma = \mathfrak{g}\mathfrak{i}' \cdot \alpha$ und folglich

$$(101) \qquad \mathfrak{g}\gamma = \mathfrak{g}\mathfrak{i}'.$$

Wir bezeichnen nun das dem Ideale $\mathfrak{g}\alpha_1$ entsprechende Ideal in $\mathfrak{o}$ mit $\mathfrak{i}_1$ und nehmen erstens an, es gehöre derselben Klasse M_0 an, wie das Ideal $\mathfrak{i}$. Da $\mathfrak{i}'$ zur entgegengesetzten Klasse M_0' gehört, so gehört $\mathfrak{i}_1 \cdot \mathfrak{i}'$ zur Klasse $M_0 M_0' = H_0$,

ist also ein Hauptideal $\mathfrak{o}\omega$ in $\mathfrak{o}$ und ω daher eine der Bedingung $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ genügende Zahl der Ordnung mit positiver Norm. Da andererseits

$$\mathfrak{g}\alpha_1 = \mathfrak{g}\mathfrak{i}_1$$

ist, folgt in Verbindung mit (101) die Gleichung

$$\mathfrak{g}\alpha_1\gamma = \mathfrak{g}\mathfrak{i}_1\mathfrak{i}' = \mathfrak{g}\mathfrak{o}\omega = \mathfrak{g}\omega,$$

aus welcher $\alpha_1\gamma$ als assoziiert zu ω, d. h.

$$\alpha_1\gamma = \varepsilon\omega$$

hervorgeht, unter ε eine Einheit verstanden, deren Norm $+1$ sein muß, da die Zahlen α_1, γ, ω positive Normen haben. Multipliziert man diese Gleichung mit α und bedenkt, daß $\alpha\gamma \equiv 1 \pmod{\mathfrak{f}}$, so ergibt sich die Kongruenz (97), welche daher notwendig ist, damit der Zahl α_1 dieselbe Klasse M_0 entspreche, wie der Zahl α.

Diese Bedingung ist aber zweitens hierfür auch ausreichend. Denn, wenn sie erfüllt ist, so folgt aus ihr mit Rücksicht auf $\alpha\gamma \equiv 1 \pmod{\mathfrak{f}}$ die andere:

$$\alpha_1\gamma\varepsilon^{-1} \equiv \omega \pmod{\mathfrak{f}}.$$

Ihr zufolge darf man, wenn zur Abkürzung

$$\alpha_1\gamma\varepsilon^{-1} = \alpha' \tag{102}$$

geschrieben wird und φ eine Zahl in $\mathfrak{f}$ bezeichnet, $\alpha' = \omega + \varphi$ setzen, woraus, da $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ gedacht wird, leicht auch $\mathfrak{o}\alpha' + \mathfrak{f} = \mathfrak{o}$ hervorgeht, während die Norm der Zahl α' den Annahmen nach positiv ist. Deshalb ist $\mathfrak{o}\alpha'$ ein Hauptideal der Ordnung. Aus (102) folgt aber

$$\mathfrak{g}\alpha' = \mathfrak{g}\alpha_1\gamma\varepsilon^{-1} = \mathfrak{g}\alpha_1\gamma$$

eine Gleichung, die auch folgendermaßen geschrieben werden kann:

$$\mathfrak{g}(\mathfrak{o}\alpha') = \mathfrak{g}\alpha_1 \cdot \mathfrak{g}\gamma = \mathfrak{g}\mathfrak{i}_1 \cdot \mathfrak{g}\mathfrak{i}' = \mathfrak{g}(\mathfrak{i}_1\mathfrak{i}')$$

und nach Nr. 2 die andere:

$$\mathfrak{o}\alpha' = \mathfrak{i}_1 \cdot \mathfrak{i}'$$

zur Folge hat. Diese lehrt aber, daß $\mathfrak{i}_1$ zur entgegengesetzten Klasse wie $\mathfrak{i}'$, d. h. zur Klasse M_0 gehört.

15. Dies vorausgeschickt, denke man sich die sämtlichen Zahlen der Ordnung $\mathfrak{o}$ (mod. $\mathfrak{f}$) in Klassen kongruenter Zahlen verteilt; genügt eine Zahl ω einer solchen Klasse der Bedingung $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$, so wird auch für jede andere Zahl ω' derselben Klasse die Bedingung $\mathfrak{o}\omega' + \mathfrak{f} = \mathfrak{o}$ erfüllt sein, da, wenn $\omega' = \omega + \varphi$ gesetzt wird, wo $\varphi \succ \mathfrak{f}$ ist, aus der ersten Gleichung, wie kurz zuvor bemerkt, die zweite folgt. Die Anzahl derartiger Klassen (mod. $\mathfrak{f}$) in der Ordnung $\mathfrak{o}$ werde wieder, wie in Nr. 11, mit $\varphi_0(\mathfrak{f})$ bezeichnet und ihre Repräsentanten, indem zur Abkürzung $v = \varphi_0(\mathfrak{f})$ gesetzt werde, mit

$$\omega_1, \omega_2, \cdots, \omega_v. \tag{103}$$

Diese Zahlen, deren Normen positiv gedacht werden dürfen, sind relativ prim zu $\mathfrak{f}$, da aus $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ stets auch $\mathfrak{g}\omega + \mathfrak{f} = \mathfrak{g}$ folgt, und sie — genauer: die durch sie repräsentierten Zahlenklassen — bilden eine Gruppe, insofern das Produkt zweier von ihnen (mod. $\mathfrak{f}$) wieder einer von ihnen kongruent sein muß; in der Tat folgt aus zwei Beziehungen

$$\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}, \quad \mathfrak{o}\omega' + \mathfrak{f} = \mathfrak{o}$$

die folgende:

$$(\mathfrak{o}\omega + \mathfrak{f}) \cdot (\mathfrak{o}\omega' + \mathfrak{f}) = \mathfrak{o} \cdot \mathfrak{o},$$

welche mit der anderen:

$$\mathfrak{o}\omega\omega' + \mathfrak{f} = \mathfrak{o}$$

übereinkommt. Demnach findet sich unter den Zahlen (103) (mod. $\mathfrak{f}$) auch die Zahl 1, sowie zu jeder der Zahlen ω_i eine zweite ihr reziproke oder entgegengesetzte Zahl ω_i' der Art, daß $\omega_i\omega_i' \equiv 1$ (mod. $\mathfrak{f}$) wird. Ist nun α irgend eine zu $\mathfrak{f}$ prime Zahl in $\mathfrak{g}$ mit positiver Norm, so sind die v Zahlen

$$\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_v,$$

deren Komplex (α) genannt werde, relativ prim zu $\mathfrak{f}$ und (mod. $\mathfrak{f}$) inkongruent; ein zweiter Komplex (α') dieser Art:

$$\alpha'\omega_1, \alpha'\omega_2, \cdots, \alpha'\omega_v$$

wird aber den Vorbemerkungen zufolge (vgl. das zur Gruppe (M_0) Gesagte) (mod. $\mathfrak{f}$) mit (α), von der Reihenfolge der Zahlen abgesehen, identisch oder völlig von (α) verschieden sein, jenachdem α' einer Zahl des Komplexes (α) kongruent ist (mod. $\mathfrak{f}$),

oder nicht. Alle zu $\mathfrak{f}$ primen Zahlen in $\mathfrak{g}$ zerfallen also (mod. $\mathfrak{f}$) in eine endliche Anzahl solcher Komplexe. Man denke sich für alle Einheiten ε, deren Norm positiv ist, die zugehörigen Komplexe gebildet, und nenne diejenigen von ihnen, welche (mod. $\mathfrak{f}$) voneinander verschieden sind,

$$(104) \qquad \begin{cases} \varepsilon_1\omega_1, & \varepsilon_1\omega_2, & \cdots, & \varepsilon_1\omega_v \\ \varepsilon_2\omega_1, & \varepsilon_2\omega_2, & \cdots, & \varepsilon_2\omega_v \\ \cdot & \cdot & \cdot & \cdot \\ \varepsilon_l\omega_1, & \varepsilon_l\omega_2, & \cdots, & \varepsilon_l\omega_v. \end{cases}$$

Auch die so erhaltenen lv zu $\mathfrak{f}$ primen und (mod. $\mathfrak{f}$) inkongruenten Zahlen bilden wieder eine Gruppe in dem Sinne, daß das Produkt von irgend zwei von ihnen wieder einer von ihnen (mod. $\mathfrak{f}$) kongruent ist; denn

$$\varepsilon_i\omega_m \cdot \varepsilon_k\omega_n$$

ist das Produkt aus einer Einheit $\varepsilon_i\varepsilon_k$ mit positiver Norm in das Produkt $\omega_m\omega_n$, welches einer der Zahlen (103) kongruent ist, und muß demnach mit einer Zahl eines der Komplexe (104) kongruent sein. Man darf daher, wie zuvor, den Schluß ziehen, daß, wenn man für jede zu $\mathfrak{f}$ prime Zahl α mit positiver Norm den größeren Komplex bildet:

$$(105) \qquad \begin{cases} \alpha\varepsilon_1\omega_1, & \alpha\varepsilon_1\omega_2, & \cdots, & \alpha\varepsilon_1\omega_v \\ \alpha\varepsilon_2\omega_1, & \alpha\varepsilon_2\omega_2, & \cdots, & \alpha\varepsilon_2\omega_v \\ \cdot & \cdot & \cdot & \cdot \\ \alpha\varepsilon_l\omega_1, & \alpha\varepsilon_l\omega_2, & \cdots, & \alpha\varepsilon_l\omega_v, \end{cases}$$

zwei solche für verschiedene Zahlen α, α_1 gebildete Komplexe (mod. $\mathfrak{f}$), abgesehen von der Reihenfolge ihrer Glieder, übereinstimmen oder durchweg voneinander verschieden sein werden, jenachdem α_1 einer Zahl des ersteren Komplexes kongruent ist oder nicht. Hieraus sieht man aber, daß die sämtlichen zu $\mathfrak{f}$ primen und (mod. $\mathfrak{f}$) inkongruenten Zahlen in $\mathfrak{g}$, deren Anzahl von uns $\varphi(\mathfrak{f})$ genannt worden ist, und deren Normen stets positiv gedacht werden dürfen, in eine endliche Menge solcher Komplexe von der Form (105) sich verteilen in der Weise, daß jede von ihnen einem und nur einem von ihnen angehören

wird. Wird die Anzahl dieser Komplexe c genannt, so folgt auf solche Weise die Beziehung

$$\varphi(\mathfrak{f}) = c \cdot lv = cl \cdot \varphi_0(\mathfrak{f}). \tag{106}$$

Nun ist aber, wie in voriger Nummer bewiesen, jede der Idealklassen M_0 einer zu $\mathfrak{f}$ relativ primen ganzen Zahl α des Körpers mit positiver Norm und daher auch einem der c Komplexe (105) in der Weise zugeordnet, daß sie genau dann für zwei Zahlen α, α_1 dieser Art dieselbe ist, wenn die Kongruenz

$$\alpha_1 \equiv \alpha \varepsilon \omega \pmod{\mathfrak{f}}$$

erfüllt ist, wo ε eine Einheit, ω eine der Beziehung $\mathfrak{o}\omega + \mathfrak{f} = \mathfrak{o}$ genügende Zahl in $\mathfrak{o}$, beide mit positiver Norm bedeuten, d. h., da $\varepsilon\omega$ notwendig (mod. $\mathfrak{f}$) mit einer der Zahlen (104) kongruent sein muß, dann und nur dann, wenn α_1 einer Zahl des Komplexes (105) kongruent, oder der der Zahl α_1 entsprechende Komplex mit dem der Zahl α entsprechenden identisch ist. Mithin muß die Anzahl der verschiedenen Klassen M_0 ebenso groß sein, wie diejenige der verschiedenen Komplexe (105), sie ist daher endlich, und, wenn wir sie, wie in voriger Nummer, mit m bezeichnen, so ist $m = c$, und so nimmt die Gleichung (106) die Gestalt

$$\varphi(\mathfrak{f}) = ml \cdot \varphi_0(\mathfrak{f})$$

und folglich die Formel (96) die folgende Form an:

$$\frac{h_0}{h} = \frac{1}{l} \cdot \frac{\varphi(\mathfrak{f})}{\varphi_0(\mathfrak{f})}. \tag{107}$$

16. Um das Verhältnis der beiden Klassenanzahlen h, h_0 vollständig zu bestimmen, bleibt noch die Zahl l zu finden. Zu diesem Zwecke bemerke man zunächst folgendes. Sind E und ε zwei beliebige Einheiten mit positiver Norm, so werden die beiden Komplexe

$$E\omega_1,\ E\omega_2,\ \cdots,\ E\omega_v$$
$$\varepsilon\omega_1,\ \varepsilon\omega_2,\ \cdots,\ \varepsilon\omega_v$$

dann und nur dann (mod. $\mathfrak{f}$) identisch miteinander sein, wenn E dem zweiten derselben angehört, d. h. wenn

$$E \equiv \varepsilon\omega_i \pmod{\mathfrak{f}}$$

ist, woraus

$$E\varepsilon^{-1} \equiv \omega_i \pmod{\mathfrak{f}}$$

und daher auch (mod. $\mathfrak{o}$), d. h. eine Gleichung

$$E\varepsilon^{-1} = \varepsilon_0 \quad \text{oder} \quad E = \varepsilon_0 \varepsilon$$

folgt, in welcher ε_0 eine Zahl der Ordnung $\mathfrak{o}$ und zwar offenbar eine Einheit derselben mit positiver Norm bedeutet. Da aber nach der Voraussetzung jeder aus einer Einheit E gebildete Komplex

$$E\omega_1,\ E\omega_2,\ \cdots,\ E\omega_v$$

mit einem der Komplexe (104) identisch ist, muß jede Einheit E des Körpers die Gestalt haben

$$E = \varepsilon_0 \varepsilon_i, \tag{108}$$

worin ε_0 eine Einheit der Ordnung (mit positiver Norm, was stets vorauszusetzen ist und deshalb weiter nicht besonders erwähnt zu werden braucht), und ε_i eine der Einheiten $\varepsilon_1,\ \varepsilon_2,\ \cdots,\ \varepsilon_l$ bedeutet; auch kann die Einheit E nur auf eine Weise die Gestalt (108) erhalten, da sie sonst (mod. $\mathfrak{f}$) mehreren der Komplexe (104) zugleich angehören würde. Man ersieht hieraus zuvörderst, daß alle Einheiten in $\mathfrak{g}$ erhalten werden — und jede von ihnen einmal — wenn man in der Formel (108) ε_0 alle Einheiten der Ordnung $\mathfrak{o}$ und ε_i die bestimmten Einheiten $\varepsilon_1,\ \varepsilon_2,\ \cdots,\ \varepsilon_l$ durchlaufen läßt. Die Einheiten des *Körpers* verteilen sich mit anderen Worten in l Komplexe, welche gebildet werden, indem man die sämtlichen Einheiten der *Ordnung* mit gewissen l Einheiten des *Körpers* multipliziert.

Da die l Produkte

$$E\varepsilon_1,\ E\varepsilon_2,\ \cdots,\ E\varepsilon_l$$

verschiedenen Komplexen angehören, mithin l Kongruenzen bestehen von der Form

$$E \cdot \varepsilon_i \equiv \varepsilon_k \cdot \omega^{(i)} \pmod{\mathfrak{f}}, \quad (i = 1, 2, \cdots, l)$$

worin die ε_k, von der Reihenfolge abgesehen, mit den Einheiten $\varepsilon_1,\ \varepsilon_2,\ \cdots,\ \varepsilon_l$ übereinstimmen müssen, die $\omega^{(i)}$ aber Zahlen in $\mathfrak{o}$ sind, so folgt für jede Einheit E die Kongruenz

$$E^l \equiv \omega^{(1)}\omega^{(2)} \cdots \omega^{(l)} \pmod{\mathfrak{f}}$$

also auch (mod. $\mathfrak{o}$), d. h. E^l ist eine in der Ordnung $\mathfrak{o}$ enthaltene Zahl, nämlich offenbar eine ihrer Einheiten.

Nach diesen Vorbemerkungen denke man sich nun sowohl die Einheiten der Ordnung wie die des Körpers durch die Fundamentaleinheiten derselben ausgedrückt. So wird allgemein

$$\varepsilon = \varepsilon_0^{x_0}\varepsilon_1^{x_1}\cdots\varepsilon_{s-1}^{x_{s-1}}, \tag{109}$$

wo $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ die Fundamentaleinheiten, ε_0 aber eine primitive Einheitswurzel vom Grade ϱ_0 ist, während ϱ_0 die Anzahl der in $\mathfrak{o}$ vorhandenen Einheitswurzeln bezeichnet. Ebenso ist

$$E = E_0^{y_0}E_1^{y_1}\cdots E_{s-1}^{y_{s-1}}, \tag{110}$$

wenn $E_1, E_2, \cdots, E_{s-1}$ die Fundamentaleinheiten, E_0 aber eine primitive Einheitswurzel des Grades ϱ ist, der die Anzahl der in $\mathfrak{g}$ vorhandenen Einheitswurzeln bezeichnet. Wenn wieder $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n-1)}$ die zu einer Zahl α konjugierten Zahlen und $l_i(\alpha)$ den reellen Teil des Logarithmus von $c_i \log(\alpha^{(i)})$ bedeuten, so folgt aus (109) und (110) für jeden Wert $i = 1, 2, \cdots, s-1$ die Formel

$$l_i(\varepsilon) = x_1 l_i(\varepsilon_1) + x_2 l_i(\varepsilon_2) + \cdots + x_{s-1} l_i(\varepsilon_{s-1}) \tag{111}$$

resp.

$$l_i(E) = y_1 l_i(E_1) + y_2 l_i(E_2) + \cdots + y_{s-1} l_i(E_{s-1}), \tag{112}$$

deren jede, da die x_i, y_i alle ganzzahligen Werte erhalten dürfen, einen bestimmten Modulus von Zahlen darstellt. Da nun jede Einheit der **Ordnung** auch eine solche des **Körpers** ist, so ist zunächst die primitive Einheitswurzel ε_0 vom Grade ϱ_0 auch eine Einheitswurzel vom Grade ϱ, somit ϱ ein Vielfaches von ϱ_0:

$$\varrho = y_0^{(0)} \cdot \varrho_0, \tag{113}$$

und

$$\varepsilon_0 = E_0^{v_0^{(0)}}. \tag{114}$$

Aus gleichem Grunde muß jede Zahl des Modulus (111) auch eine Zahl des Modulus (112) oder jener in diesem enthalten und also beider kleinstes gemeinsames Vielfache sein. Andererseits ist, weil E^l eine Einheit der Ordnung ist, das l-fache jeder Zahl des Modulus (112) eine solche des Modulus (111). Nach Kap. 2, Nr. 6 hat demnach dieser eine Basis, welche in Analogie mit den dortigen Formeln (53) folgendermaßen ausgedrückt werden kann:

$$(115)\quad \begin{cases} l_i(\eta_1) = y_1^{(1)} \cdot l_i(E_1) \\ l_i(\eta_2) = y_1^{(2)} \cdot l_i(E_1) + y_2^{(2)} \cdot l_i(E_2) \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ l_i(\eta_{s-1}) = y_1^{(s-1)} \cdot l_i(E_1) + y_2^{(s-1)} \cdot l_i(E_2) + \cdots + y_{s-1}^{(s-1)} \cdot l_i(E_{s-1}), \end{cases}$$

wo die $y_k^{(i)}$ ganze Zahlen bedeuten, unter denen $y_1^{(1)}, y_2^{(2)}, \cdots, y_{s-1}^{(s-1)}$ positiv sind; $\eta_1, \eta_2, \cdots, \eta_{s-1}$ bezeichnen Einheiten der Ordnung. Demnach kann die Formel (111) auch durch die andere ersetzt werden:

$$(116)\quad l_i(\varepsilon) = z_1 l_i(\eta_1) + z_2 l_i(\eta_2) + \cdots + z_{s-1} l_i(\eta_{s-1}),$$

in welcher die z_i alle rationalen ganzen Zahlen bedeuten. Da die Determinante der Gleichungen (115) gleich

$$y_1^{(1)} \cdot y_2^{(2)} \cdots y_{s-1}^{(s-1)}$$

also positiv ist und aus ihnen sich die Gleichung

$$(117)\quad |l_i(\eta_k)| = y_1^{(1)} y_2^{(2)} \cdots y_{s-1}^{(s-1)} \cdot |l_i(E_k)|$$

ergibt, so bilden die Einheiten $\eta_1, \eta_2, \cdots \eta_{s-1}$ ein System von unabhängigen Einheiten in $\mathfrak{o}$, die sogar Fundamentaleinheiten sein müssen, denn analog mit (116) gelten für die Fundamentaleinheiten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{s-1}$ Gleichungen von der Gestalt

$$l_i(\varepsilon_k) = z_{1k} l_i(\eta_1) + z_{2k} l_i(\eta_2) + \cdots + z_{s-1,k} l_i(\eta_{s-1}),$$
$$(k = 1, 2, \cdots, s-1)$$

aus denen $|l_i(\varepsilon_k)|$ als ganzzahliges Vielfaches von $|l_i(\eta_k)|$ hervorgeht, was die Wahrheit der Aussage beweist. Man darf daher in Übereinstimmung mit (116)

$$(118)\quad \varepsilon = \varepsilon_0^{z_0} \cdot \eta_1^{z_1} \eta_2^{z_2} \cdots \eta_{s-1}^{z_{s-1}}$$

setzen. Andererseits ist aber ε als eine auch zu $\mathfrak{g}$ gehörige Einheit von der Form

$$(119)\quad \varepsilon = E_0^{u_0} \cdot E_1^{u_1} E_2^{u_2} \cdots E_{s-1}^{u_{s-1}}.$$

Desgleichen können auch die Einheiten $\eta_1, \eta_2, \cdots, \eta_{s-1}$ der Ordnung durch die Fundamentaleinheiten des Körpers ausgedrückt werden, und man findet entsprechend den Gleichungen (115)

$$\begin{aligned} \eta_1 &= E_0^{y_0(1)} E_1^{y_1(1)} \\ \eta_2 &= E_0^{y(2)} \cdot E_1^{y_1(2)} \cdot E_2^{y_2(2)} \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \eta_{s-1} &= E_0^{y_0(s-1)} \cdot E_1^{y_1(s-1)} \cdot E_2^{y_2(s-1)} \cdots E_{s-1}^{y_{s-1}(s-1)}, \end{aligned}$$

wo $y_0^{(1)}, y_0^{(2)}, \cdots, y_0^{(s-1)}$ nicht negative ganze Zahlen bedeuten, welche kleiner sind als ϱ. Werden diese Ausdrücke in (118) eingesetzt und die entstehende Formel mit (119) verglichen, so gehen die Gleichungen:

$$(120)\quad \begin{cases} u_0 &= z_0 y_0^{(0)} + z_1 y_0^{(1)} + z_2 y_0^{(2)} + \cdots + z_{s-1} y_0^{(s-1)} \\ u_1 &= \qquad\quad z_1 y_1^{(1)} + z_2 y_1^{(2)} + \cdots + z_{s-1} y_1^{(s-1)} \\ u_2 &= \qquad\qquad\qquad z_2 y_2^{(2)} + \cdots + z_{s-1} y_2^{(s-1)} \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{s-1} &= \qquad\qquad\qquad\qquad\qquad z_{s-1} y_{s-1}^{(s-1)} \end{cases}$$

hervor, in denen offenbar die ganzen Zahlen $z_0, z_1, z_2, \cdots, z_{s-1}$ auf eine ganz bestimmte Art so gewählt werden können, daß successive die Differenzen

$$y_{s-1} - u_{s-1},\; y_{s-2} - u_{s-2},\; \cdots,\; y_2 - u_2,\; y_1 - u_1,\; y_0 - u_0$$

nicht negativ und kleiner werden als resp.

$$y_{s-1}^{(s-1)},\; y_{s-2}^{(s-2)},\; \cdots,\; y_2^{(2)},\; y_1^{(1)},\; y_0^{(0)}.$$

Nun ist

$$(121)\qquad E = H \cdot \varepsilon,$$

wenn

$$(122)\qquad H = E_0^{y_0 - u_0} \cdot E_1^{y_1 - u_1} E_2^{y_2 - u_2} \cdots E_{s-1}^{y_{s-1} - u_{s-1}}$$

gesetzt wird. Somit folgert man, daß für jede Einheit E des Körpers eine ganz bestimmte Einheit ε der Ordnung vorhanden ist von der Beschaffenheit, daß in der Formel (121) die Exponenten der Einheit H in der zuvor angegebenen Weise begrenzt sind; solcher Einheiten H gibt es offenbar

$$(123)\qquad y = y_0^{(0)} y_1^{(1)} y_2^{(2)} \cdots y_{s-1}^{(s-1)}.$$

Demnach können sämtliche Einheiten des *Körpers* in y Komplexe von der Form (121) verteilt werden, deren Glieder man erhält, wenn man ε sämtliche Einheiten der *Ordnung* durchlaufen läßt. Da aber H notwendig in einem der l Komplexe, welche am Anfang dieser Nummer besprochen worden sind, enthalten, jeder der Komplexe (121) also mit einem dieser letztern identisch sein muß und umgekehrt, so folgt die Gleichheit der beiden Anzahlen

$$l = y$$

d. h. mit Beachtung der Beziehungen (123), (117) und (113) die Gleichung

$$l = y_0^{(0)} \cdot \frac{|\, l_i(\eta_k) \,|}{|\, l_i(E_k) \,|} = \frac{\varrho \cdot |\, l_i(\eta_k) \,|}{\varrho_0 \cdot |\, l_i(E_k) \,|} = \frac{Q_0}{Q},$$

wenn mit Q, Q_0 dieselben Quotienten bezeichnet werden, wie in Formel (92). Durch Einsetzen dieses Wertes der Zahl l in Formel (107) entsteht endlich die Gleichung

$$\frac{h_0}{h} = \frac{Q}{Q_0} \cdot \frac{\varphi(\mathfrak{f})}{\varphi_0(\mathfrak{f})},$$

welche mit jener auf analytischem Wege bereits ermittelten Formel (92) übereinkommt.

Zehntes Kapitel.

Die zerlegbaren Formen.

1. Schon im fünften Kapitel hat sich gezeigt, in wie innigem Zusammenhange die Theorie der Zahlen eines quadratischen Körpers mit der Lehre von den quadratischen Formen mit einer gewissen gegebenen Determinante steht. Gleiches gilt aber für die Zahlen eines beliebigen Körpers n^{ten} Grades und bestimmte zerlegbare Formen dieses Grades mit n Unbestimmten, und der Vollständigkeit wegen darf nicht unterlassen werden, dies wenigstens andeutungsweise hier auseinanderzusetzen.

Unter einer Form n^{ten} Grades mit n Unbestimmten u_1, $u_2, \cdots, u_n$ versteht man bekanntlich jede ganze homogene Funktion n^{ter} Dimension dieser Unbestimmten. Eine solche Form heißt zerlegbar, wenn sie als Produkt von n Linearformen darstellbar ist. Sei

$$(1) \qquad F(u_1, u_2, \cdots, u_n) = U_1 \cdot U_2 \cdots U_n$$

eine zerlegbare Form n^{ten} Grades, also

$$(2) \qquad U_i = \gamma_{i1} u_1 + \gamma_{i2} u_2 + \cdots + \gamma_{in} u_n, \quad (i = 1, 2, \cdots, n)$$

wo die γ_{ik} irgend welche algebraische Zahlen bedeuten. Die

sogenannte Funktionaldeterminante der Ausdrücke $U_1, U_2, \cdots U_n$ in bezug auf die Unbestimmten $u_1, u_2, \cdots, u_n$, in Zeichen:

$$\left| \frac{\partial U_i}{\partial u_k} \right|,$$

ist nichts anderes als die Determinante $|\gamma_{ik}|$ der Gleichungen (2); ihr Quadrat soll die Diskriminante der Form F genannt werden, in Zeichen:

$$\Delta(F) = |\gamma_{ik}|^2. \tag{3}$$

Die Zerlegung der Form F in Linearfaktoren ist offenbar keine nur eindeutig mögliche, da man statt (1) auch

$$F(u_1, u_2, \cdots, u_n) = c_1 U_1 \cdot c_2 U_2 \cdots c_n U_n$$

setzen könnte, wo die c_i beliebige Konstanten, vorausgesetzt nur, daß ihr Produkt gleich 1. Doch sieht man nach der Definition von $\Delta(F)$ sogleich ein, daß wegen dieser notwendigen Voraussetzung die Diskriminante der Form völlig bestimmt ist. Da sich aus (1) und (2) die Beziehungen

$$\frac{\partial \log \cdot F}{\partial u_r} = \sum_i \frac{\gamma_{ir}}{U_i}$$

$$\frac{\partial^2 \log \cdot F}{\partial u_r \partial u_s} = - \sum_i \frac{\gamma_{ir} \gamma_{is}}{U_i^2}$$

herausstellen, so ergibt sich nach dem Multiplikationssatze für Determinanten die Gleichung:

$$\left| \frac{\partial^2 \log \cdot F}{\partial u_r \partial u_s} \right| = \frac{(-1)^n \cdot \Delta(F)}{F^2}. \tag{4}$$

Andererseits aber findet man

$$\frac{\partial^2 \log \cdot F}{\partial u_r \partial u_s} = \frac{1}{F^2} \left(F \cdot \frac{\partial^2 F}{\partial u_r \partial u_s} - \frac{\partial F}{\partial u_r} \cdot \frac{\partial F}{\partial u_s} \right).$$

Wenn man nun in der Determinante

$$(F) = \begin{vmatrix} F, & \frac{\partial F}{\partial u_1}, & \frac{\partial F}{\partial u_2}, & \cdots\cdots, & \frac{\partial F}{\partial u_n} \\ \frac{\partial F}{\partial u_1}, & \frac{\partial^2 F}{\partial u_1 \partial u_1}, & \frac{\partial^2 F}{\partial u_1 \partial u_2}, & \cdots, & \frac{\partial^2 F}{\partial u_1 \partial u_n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \frac{\partial F}{\partial u_n}, & \frac{\partial^2 F}{\partial u_n \partial u_1}, & \frac{\partial^2 F}{\partial u_n \partial u_2}, & \cdots, & \frac{\partial^2 F}{\partial u_n \partial u_n} \end{vmatrix} \tag{5}$$

die letzten n Reihen mit F multipliziert und dann die erste Reihe, bezw. mit $\frac{\partial F}{\partial u_1}, \frac{\partial F}{\partial u_2}, \cdots, \frac{\partial F}{\partial u_n}$ multipliziert, von ihnen abzieht, so verschwinden bis auf das Anfangsglied die Glieder der ersten Kolonne, und die Gleichung (5) verwandelt sich in diese:

$$F^n \cdot (F) = F^{2n+1} \cdot \left| \frac{\partial^2 \log \cdot F}{\partial u_r \partial u_s} \right|$$

oder

$$(F) = F^{n+1} \cdot \left| \frac{\partial^2 \log \cdot F}{\partial u_r \partial u_s} \right|,$$

welche dann durch die Gleichung (4) in die folgende übergeht:

$$(F) = (-1)^n \cdot F^{n-1} \cdot \varDelta(F). \tag{6}$$

Ist die Funktion F eine ganzzahlige und t ihr Teiler, d. i. der größte gemeinsame Teiler ihrer Koeffizienten (s. Kap. 6, Nr. 3), also (nach derselben Stelle) t^{n-1} derjenige von F^{n-1}, so wird (F) gewiß durch t^{n+1} teilbar sein, da alle Elemente der Determinante (5) den Teiler t haben müssen; demnach muß $\varDelta(F)$ dann durch t^2 aufgehen.

Man ersieht ferner aus der Definition der Diskriminante der Form, daß, so oft c eine Konstante ist, die Gleichung

$$\varDelta(cF) = c^2 \cdot \varDelta(F) \tag{7}$$

stattfinden muß, gleichviel, ob F eine ganzzahlige Form ist, oder nicht. —

Nach diesen allgemeinen Bemerkungen über zerlegbare Formen wenden wir uns speziell zur Betrachtung **der zerlegbaren Formen eines Körpers $\mathfrak{K}$ n^{ten} Grades.** Man nennt so eine Form $F(u_1, u_2, \cdots, u_n)$, wenn sie als Norm einer Linearform

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n \tag{8}$$

darstellbar ist, deren Koeffizienten $\alpha_1, \alpha_2, \cdots, \alpha_n$ ganze oder gebrochene Zahlen des Körpers sind; ihre eigenen Koeffizienten werden stets rationale Zahlen sein. Jedoch ist hier eine Einschränkung vonnöten. Wenn nämlich die Koeffizienten α_i zugleich auch Zahlen eines Körpers $\mathfrak{K}'$ geringeren Grades m wären, welcher dann als in jenem enthalten gedacht werden dürfte, sodaß m ein Teiler von n oder $n = m\nu$ wäre, so würden die n mit bezug auf $\mathfrak{K}$ konjugierten Werte eines jeden

der Koeffizienten α_i zu je ν einander gleich, nämlich gleich den m in bezug auf $\mathfrak{K}'$ konjugierten Werten von α_i sein (s. Kap. 1, Nr. 13), also würde

$$N_{\mathfrak{K}}(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n) = N_{\mathfrak{K}'}(\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n)^\nu,$$

wo nun schon die Norm zur Rechten eine homogene ganze Funktion der u_i vom Grade m mit rationalen Koeffizienten sein würde; mithin wäre die Form F reduktibel, d. h. sie zerfiele in Faktoren geringeren Grades mit ebenfalls rationalen Koeffizienten. Setzen wir daher fest, sie solle im Gegenteil **irreduktibel** gedacht werden, so können die α_i nicht sämtlich einem Körper geringeren Grades als der des Körpers $\mathfrak{K}$ angehörig sein. Ferner aber würde, wenn die n Koeffizienten $\alpha_1, \alpha_2, \cdots, \alpha_n$ nicht rational unabhängig voneinander wären, sondern z. B. α_n durch die übrigen mit rationalen Koeffizienten ausdrückbar wäre:

$$\alpha_n = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_{n-1}\alpha_{n-1},$$

die Linearform (8) in die folgende übergehen:

$$\alpha_1(u_1 + c_1 u_n) + \alpha_2(u_2 + c_2 u_n) + \cdots + \alpha_{n-1}(u_{n-1} + c_{n-1}u_n),$$

welche, ebenso wie dann die Form F nur noch $n-1$ Unbestimmte

$$u_1' = u_1 + c_1 u_n, \quad u_2' = u_2 + c_2 u_n, \cdots, u'_{n-1} = u_{n-1} + c_{n-1}u_n$$

enthielte. Wird daher endlich noch festgesetzt, daß die n Unbestimmten oder Veränderlichen der Form **unabhängig** sein sollen, so müssen die Koeffizienten $\alpha_1, \alpha_2, \cdots, \alpha_n$ rational unabhängig sein, womit denn auch zugleich ihre Zugehörigkeit zu einem Körper geringeren als n^{ten} Grades unmöglich gemacht wird.

Wir definieren demnach bestimmter als zerlegbare Form eines Körpers $\mathfrak{K}$ n^{ten} Grades eine irreduktible Form vom Grade n mit n unabhängigen Variabeln u_i, welche als Norm einer Linearform (8) mit in $\mathfrak{K}$ enthaltenen Koeffizienten α_i darstellbar ist. Diese Koeffizienten bilden dann stets eine Basis des Körpers. Die Form wird primitiv oder eine Einheitsform genannt, wenn sie ganzzahlige Koeffizienten hat, deren größter gemeinsamer Teiler gleich 1 ist.

2. **Vor allem soll festgestellt werden, in welcher Beziehung die Diskriminante einer zerlegbaren Form des Körpers zu seiner Grundzahl steht.**

Sei $E(u_1, u_2, \cdots, u_n)$ eine derartige zerlegbare Einheitsform n^{ten} Grades mit n Veränderlichen u_i, und U_1 irgend einer ihrer Linearfaktoren. Die Koeffizienten des letztern gehören dem eben Gesagten zufolge einem Körper n^{ten} Grades an, und bilden eine Basis desselben, brauchen aber keine ganzen Zahlen dieses Körpers zu sein. Indessen gibt es nach Kap. 4, Nr. 2 für jede der Basiszahlen eine ganze, ja sogar eine rationale ganze Zahl des Körpers, durch welche multipliziert sie zu einer ganzen Zahl wird; es gibt daher auch eine ganze Zahl γ des Körpers (z. B. das Produkt jener Multiplikatoren), durch welche multipliziert die sämtlichen Koeffizienten von U_1 zu ganzen Zahlen des Körpers werden, welche $\alpha_1, \alpha_2, \cdots, \alpha_n$ heißen mögen, sodaß

$$(9) \qquad \gamma \cdot U_1 = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

gesetzt werden kann. Diese Linearform mit algebraisch ganzen Koeffizienten nennen wir

$$(10) \qquad \mathrm{F} = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n;$$

sie ist die Linearform des Modulus

$$(11) \qquad \mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n],$$

dessen sämtliche Zahlen aus ihr erhalten werden, wenn den Unbestimmten u_i alle rationalen ganzzahligen Werte beigelegt werden. Der Quotient $\frac{\mathfrak{m}}{\mathfrak{m}}$ ist nach Kap. 2, Nr. 2 eine Ordnung ganzer Zahlen des Körpers, welche $\mathfrak{o}$ genannt werde, und es ist $\mathfrak{o}\mathfrak{m} \succ \mathfrak{m}$. Sind daher $\omega_1, \omega_2, \cdots, \omega_n$ eine Basis von $\mathfrak{o}$, so werden die sämtlichen Produkte $\omega_i \cdot \alpha_k$ Zahlen des Modulus $\mathfrak{m}$, also als lineare Funktionen der α_i mit ganzzahligen Koeffizienten ausdrückbar sein, daher gehen aus (10) Gleichungen hervor von der Form

$$(12) \qquad \mathrm{F} \cdot \omega_i = U_{i1}\alpha_1 + U_{i2}\alpha_2 + \cdots + U_{in}\alpha_n, \quad (i = 1, 2, \cdots, n)$$

in denen die U_{ik} homogene lineare Funktionen der u_i mit ganzzahligen Koeffizienten bedeuten. Die Determinante

(13) $$U = | U_{ik} |$$

dieser n Gleichungen ist also eine homogene ganze und ganzzahlige Funktion der Unbestimmten u_i vom Grade n. Da die ω_i als Basis von $\mathfrak{o}$ auch eine Basis des Körpers bilden, müssen Gleichungen bestehen von der Form

(14) $$\alpha_i = g_{i1}\omega_1 + g_{i2}\omega_2 + \cdots + g_{in}\omega_n, \quad (i = 1, 2, \cdots, n)$$

deren Determinante nach ihrem Absolutwerte den Quotienten $\frac{(\mathfrak{o}, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o})}$ ausdrückt (s. Ende von Kap. 2), in Zeichen:

(15) $$\pm | g_{ik} | = \frac{(\mathfrak{o}, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o})};$$

durch Einsetzen der Ausdrücke (14) aber in (12) nehmen die letzteren Gleichungen die Gestalt an:

(12ᵃ) $$\mathrm{F} \cdot \omega_i = \sum_{k, h} U_{ik} g_{kh} \cdot \omega_h, \quad (i = 1, 2, \cdots, n)$$

woraus nach Kap. 1, Nr. 8 für jedes ganzzahlige Wertsystem der u_i, d. h. für die entsprechende aus F entstehende Zahl α des Modulus $\mathfrak{m}$

$$N(\alpha) = | U_{ik} | \cdot | g_{kh} |$$

zu erschließen ist. Da somit für die unendlich vielen ganzzahligen Werte jeder der Unbestimmten u_i die Gleichung

(16) $$N(\mathrm{F}) = | g_{ik} | \cdot U$$

erfüllt ist, folgt ihr identisches Bestehen.

Die durch die Formel (13) definierte Funktion U ist hiernach eine zerlegbare Form, welche wegen ihrer Herleitung aus dem Modulus $\mathfrak{m}$ die dem letzteren entsprechende Form heißen soll.

Der Modulus $\mathfrak{m}$ braucht kein Ideal des Körpers zu sein; jedenfalls ist aber der allgemeinere, im Sinne von Kap. 3, Nr. 1 genommene Modulus

$$\mathfrak{a} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$$

solch' ein Ideal, auch wenn nicht gerade $\alpha_1, \alpha_2, \cdots, \alpha_n$ eine Basis desselben ausmachen. Da es der Inhalt der Linearform

F ist, so ist nach Kap. 7, Nr. 5 $\mathfrak{N}(\mathfrak{a})$ der Teiler ihrer Norm $N(\mathrm{F})$. Da nun

$$N(\gamma) \cdot E = N(\mathrm{F})$$

und E eine Einheitsform ist, ergibt sich die Gleichheit von $N(\gamma)$ und $\mathfrak{N}(\mathfrak{a})$ und die Gleichung

$$N(\mathrm{F}) = \mathfrak{N}(\mathfrak{a}) \cdot E. \tag{17}$$

Wenn aber $\beta_1, \beta_2, \cdots, \beta_n$ eine **Basis** von $\mathfrak{a}$ bedeuten, sodaß n ganzzahlige Gleichungen

$$\alpha_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \cdots + a_{in}\beta_n \tag{18}$$
$$(i = 1, 2, \cdots, n)$$

bestehen, während andererseits die β_i mittels n ganzzahliger Gleichungen von der Form

$$\beta_i = b_{i1}\gamma_1 + b_{i2}\gamma_2 + \cdots + b_{in}\gamma_n \tag{19}$$
$$(i = 1, 2, \cdots, n)$$

durch die Basiszahlen γ_i für die Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen des Körpers ausgedrückt werden können, so folgen daraus n Gleichungen von der Gestalt:

$$\alpha_i = c_{i1}\gamma_1 + c_{i2}\gamma_2 + \cdots + c_{in}\gamma_n, \tag{20}$$
$$(i = 1, 2, \cdots, n)$$

deren von Null verschiedene Determinante

$$| c_{ik} | = | a_{ik} | \cdot | b_{ik} | \tag{21}$$

ist. Ferner findet sich nach der Definition der Formendiskriminante

$$\varDelta(N(\mathrm{F})) = \varDelta(\mathfrak{m}) = | a_{ik} |^2 \cdot | b_{ik} |^2 \cdot \varDelta(\mathfrak{g}),$$

während

$$| b_{ik} | = (\mathfrak{g}, \mathfrak{a}) = \mathfrak{N}(\mathfrak{a})$$

ist. Da andererseits wegen (17) mit Rücksicht auf (7)

$$\varDelta(N(\mathrm{F})) = \mathfrak{N}(\mathfrak{a})^2 \cdot \varDelta(E)$$

gefunden wird, gewinnt man durch Vergleichung der beiden Ausdrücke für $\varDelta(N(\mathrm{F}))$ die Beziehung, um die es sich handelt:

$$\varDelta(E) = | a_{ik} |^2 \cdot \mathrm{D}, \tag{22}$$

wo $\mathrm{D} = \varDelta(\mathfrak{g})$ die Grundzahl des Körpers bezeichnet.

Die Grundzahl des Körpers, dem eine zerlegbare Einheitsform zugehört, ist also stets ein Teiler ihrer

Diskriminante und beider Verhältnis ist eine ganze Quadratzahl. Da hiernach für einen gegebenen Wert der Diskriminante $\Delta(E)$ die Zahl D nur eine endliche Menge von Werten haben kann, und da zu einer gegebenen Grundzahl nur eine endliche Menge von Körpern n^{ten} Grades vorhanden ist (Kap. 8, Nr. 7), so verteilen sich sämtliche zerlegbaren Einheitsformen n^{ten} Grades mit gegebener Diskriminante auf eine endliche Anzahl von Körpern n^{ten} Grades. Umgekehrt sind die Diskriminanten aller zerlegbaren Einheitsformen, welche zu einem bestimmten Körper gehören, quadratische Vielfache seiner Grundzahl. Soll die Diskriminante einer solchen Einheitsform der Grundzahl des Körpers gleich sein, so ist dafür nach der Gleichung (22) notwendig und hinreichend, daß

$$|a_{ik}| = \pm 1$$

sei, wo stets das positive Vorzeichen gedacht werden darf, wenn die Reihenfolge der Basiszahlen β_i passend gewählt wird; dies kommt aber nach (21) auf die Bedingung

$$|c_{ik}| = \mathfrak{N}(\mathfrak{a})$$

hinaus, welche die Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_n$ als eine Basis des Ideals $\mathfrak{a}$ kennzeichnet (vgl. Kap. 4, Nr. 7). Hiernach darf man sagen: Jeder zerlegbaren Einheitsform E, welche einem bestimmten Körper $\mathfrak{K}$ n^{ten} Grades zugehört, und eine seiner Grundzahl gleiche Diskriminante hat, entspricht ein Ideal $\mathfrak{a}$ des Körpers, nämlich ein Ideal

$$[\alpha_1, \alpha_2, \cdots, \alpha_n],$$

dessen Linearform F ist und welches durch die Form E in der am Anfang dieser Nummer angegebenen Weise bestimmt ist. Umgekehrt entspricht jedem Ideale $\mathfrak{a}$ des Körpers eine zu ihm gehörige Einheitsform mit der Diskriminante D, da die nach Kap. 7, Nr. 5 durch die Formel (17) gelieferte Form E eine solche ist.[1])

---

1) Die Zugehörigkeit der Form zum Körper wird jedoch hier in etwas weiterem Sinne gedacht. Daß die Form E in Formel (17) zerlegbar ist, leuchtet ohne weiteres ein, doch werden im allgemeinen die Koeffizienten ihres Linearfaktors keine Zahlen, sondern nur Ideale

3. Dies Letztere läßt sich statt aus der angezogenen Nummer folgendermaßen erkennen. Ist der Modulus (11) ein Ideal, so ist seine Ordnung $\mathfrak{o} = \mathfrak{g}$ und die Zahlen ω_i eine Basis von $\mathfrak{g}$, mithin werden die Koeffizienten g_{ik} in (14) ganze rationale Zahlen und bei geeigneter Reihenfolge der Zahlen ω_i

$$|g_{ik}| = (\mathfrak{g}, \mathfrak{m}) = \mathfrak{N}(\mathfrak{m}).$$

Dadurch nimmt die Gleichung (16) die Gestalt an:

$$N(\mathrm{F}) = \mathfrak{N}(\mathfrak{m}) \cdot U \tag{23}$$

und es ist zunächst zu zeigen, daß die Form U eine Einheitsform ist. Denkt man sich hierzu die Unbestimmten u_i durch irgend welche rationalen ganzen Zahlen ersetzt, wodurch F in eine Zahl α des Ideals (11) übergeht, und bedenkt, daß mit α zugleich das Ideal $\mathfrak{g}\alpha$ in $\mathfrak{m}$ enthalten ist, also $\mathfrak{g}\alpha = \mathfrak{m} \cdot \mathfrak{n}$ gesetzt werden kann, wo $\mathfrak{n}$ ein Ideal des Körpers bezeichnet, so wird

$$\pm N(\alpha) = \mathfrak{N}(\mathfrak{g}\alpha) = \mathfrak{N}(\mathfrak{m}) \cdot \mathfrak{N}(\mathfrak{n})$$

und es findet sich durch Verbindung mit der voraufgehenden Gleichung

$$U = \pm \mathfrak{N}(\mathfrak{n}). \tag{24}$$

Nun kann aber (nach Kap. 6, Nr. 17) das Ideal $\mathfrak{n}$, welches mit $\mathfrak{m}$ zusammengesetzt ein Ideal $\mathfrak{g}\alpha$ hervorbringt, stets so gewählt werden, daß es zu einem gegebenen Ideale, z. B. zum Ideale $\mathfrak{g}k$, wo k eine beliebig gegebene rationale ganze Zahl sei, relativ prim ist. Denkt man also die ganzzahligen Werte der Unbestimmten u_i als diejenigen, welche die entsprechende, stets in $\mathfrak{m}$ enthaltene Zahl α hervorbringen, so wird der zugehörige Wert der Form U nach (24) ebenfalls relativ prim zu k (vgl. Kap. 6, Nr. 18), d. i. zu jeder beliebigen ganzen Zahl, also U notwendig primitiv sein. — Die Diskriminante dieser Einheitsform endlich, die, wie $N(\mathrm{F})$ selbst im Körper zerlegbar ist (s. die vorige Anmerkung), wird durch die aus (23) mit Rücksicht auf (7) hervorgehende Beziehung

---

des Körpers sein. Später wird gezeigt werden, daß $\mathfrak{N}(\mathfrak{a}) = N(\mathfrak{j})$ gesetzt werden kann, wo $\mathfrak{j}$ ein Ideal ist; demnach wird der Linearfaktor von E gleich $\frac{F}{\mathfrak{j}}$ sein.

$$\Delta(N(\mathrm{F})) = \mathfrak{N}(\mathfrak{m})^2 \cdot \Delta(U)$$

bestimmt, und findet sich, da andererseits

$$\Delta(N(\mathrm{F})) = \Delta(\mathfrak{m}) = \mathfrak{N}(\mathfrak{m})^2 \cdot \Delta(\mathfrak{g})$$

ist,

$$\Delta(U) = \Delta(\mathfrak{g}) = \mathrm{D},$$

und somit ist U eine der mit E bezeichneten Einheitsformen mit der Diskriminante D, welche, da sie durch das Ideal (11) völlig bestimmt ist, als diesem entsprechend zu bezeichnen ist; wir setzen daher wieder das Zeichen E an Stelle von U.

Die Werte, welche diese Form E annimmt, wenn in ihr den Unbestimmten ganzzahlige Werte beigelegt werden, heißen die durch die Form darstellbaren Zahlen. Um näher festzustellen, welche Zahlen dies sind, erwäge man, daß dem oben Gesagten gemäß jedem ganzzahligen Wertsysteme der u_i vermittelst (10) eine bestimmte Zahl α des Ideals $\mathfrak{m}$ entspricht, welcher wieder durch die Formel $\mathfrak{g}\alpha = \mathfrak{m} \cdot \mathfrak{n}$ ein bestimmtes Ideal $\mathfrak{n}$ zugeordnet ist von der Beschaffenheit, daß E durch jenes Wertsystem den Wert $+\mathfrak{N}(\mathfrak{n})$ oder $-\mathfrak{N}(\mathfrak{n})$ erhält, je nachdem $N(\alpha)$ positiv oder negativ ist. Wenn hieraus folgt, daß durch E nur ganze rationale Zahlen dieser Art darstellbar sind, so können sie aber auch sämtlich durch E dargestellt werden, da jedem Ideale $\mathfrak{n}$, für welches $\mathfrak{m} \cdot \mathfrak{n}$ ein Ideal $\mathfrak{g}\alpha$ wird, eine bestimmte in $\mathfrak{m}$ enthaltene Zahl α, also auch ein bestimmtes ganzzahliges Wertsystem der u_i entspricht, für welches das oben Gesagte zutrifft, nämlich E den Wert $\pm\mathfrak{N}(\mathfrak{n})$ annimmt. — Zu den gedachten Idealen $\mathfrak{n}$ zählen stets die sämtlichen Ideale der zur Klasse C, zu der das Ideal $\mathfrak{m}$ gehört, entgegengesetzten Klasse C', für welche nämlich $\mathfrak{m} \cdot \mathfrak{n}$ ein Hauptideal $\mathfrak{g}\alpha$, d. i. α eine Zahl mit positiver Norm ist. Die Normen aller Ideale dieser Klasse C' sind also durch die Form E darstellbar. Gibt es im Ideale $\mathfrak{m}$ keine Zahlen mit negativer Norm, so sind die bezeichneten Normen auch die einzigen durch E darstellbaren Zahlen. Wenn aber Zahlen α mit negativer Norm in $\mathfrak{m}$ vorhanden sind, so bilden diejenigen Ideale $\mathfrak{n}$, für welche $\mathfrak{g}\alpha = \mathfrak{m} \cdot \mathfrak{n}$ ist, eine im allgemeinen von C' verschiedene Klasse C'', die jener nur halbäquivalent ist, während die der Zahl α entsprechenden Werte der Un-

bestimmten u_i eine Darstellung von $-\mathfrak{N}(\mathfrak{n})$ durch E liefern. In diesem Falle sind also die durch E darstellbaren positiven Zahlen die Normen der Ideale der Klasse C', die durch E darstellbaren negativen Zahlen die Normen der Ideale der Klasse C'' mit negativem Vorzeichen genommen. Sind insbesondere Einheiten mit negativer Norm vorhanden, so folgt wegen

$$\mathfrak{g}(\varepsilon\alpha) = \mathfrak{g}(\alpha) = \mathfrak{m} \cdot \mathfrak{n},$$

daß die der Zahl $\varepsilon\alpha$ entsprechenden Werte der Unbestimmten u_i eine Darstellung auch der negativ genommenen Norm von $\mathfrak{n}$ hervorbringen. In diesem besonderen Falle sind die durch E darstellbaren Zahlen die positiv und negativ genommenen Normen aller Ideale der Klasse C'.

Ist $\pm m$ irgend eine der durch E darstellbaren ganzen Zahlen, so muß m dem Gesagten zufolge die Norm eines der Ideale der Klasse C' oder der Klasse C'' sein; aber es gibt unendlich viel einander assoziierte Ideale der einen wie der anderen dieser Klassen, deren Normen gleich m sind, und demgemäß stets unendlich viel Darstellungen von $\pm m$ durch die Form E, die zu einer Gruppe vereint werden können. Ist nämlich

$$\mathfrak{n}' = \varepsilon\mathfrak{n}$$

und

$$\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{g}\alpha,$$

so ist auch

$$\mathfrak{m} \cdot \mathfrak{n}' = \mathfrak{g}(\varepsilon\alpha),$$

wo ε eine Einheit bezeichnet, und jeder solchen Einheit entspricht zugleich mit der in $\mathfrak{m}$ enthaltenen Zahl $\varepsilon\alpha$ ein Wertsystem der Unbestimmten u_i, durch welches die Zahl $\pm m = \pm\mathfrak{N}(\mathfrak{n}) = \pm\mathfrak{N}(\mathfrak{n}')$ mit gleichem Vorzeichen, wie es der Zahl $N(\alpha)$ zukommt, dargestellt wird, wenn die Einheit ε mit positiver Norm gedacht wird.

Man erkennt in diesen Aussprüchen über die Darstellung durch die zerlegbare Form E die völligste Analogie mit den bekannten Sätzen, nach welchen die Darstellungen durch die binären quadratischen Formen in Darstellungsgruppen, die zu bestimmten Kongruenzwurzeln gehören, verteilt werden.

4. Diese Analogie zwischen den allgemeineren und den genannten besonderen Formen läßt sich aber viel weiter ver-

folgen. Wenn man die Basis des Ideals $\mathfrak{m}$ durch irgend eine andere ersetzt, indem man n Gleichungen mit ganzzahligen Koeffizienten aufstellt:

$$\beta_i = a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n, \quad (i = 1, 2, \cdots, n) \tag{25}$$

deren Determinante, welche positiv gedacht werden darf und soll, gleich 1 ist, so geht $\mathfrak{m}$ über in den Modulus

$$\mathfrak{m} = [\beta_1, \beta_2, \cdots, \beta_n];$$

ist dann

$$\Phi = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

so erhält man, entsprechend der Gleichung (23), diese andere:

$$N(\Phi) = \mathfrak{N}(\mathfrak{m}) \cdot V, \tag{26}$$

wo V eine zerlegbare Einheitsform des Körpers mit der Diskriminante D sein wird. Da aber Φ durch Einsetzen der Ausdrücke (25) in

$$\mathrm{F} = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

übergeht, vorausgesetzt, daß

$$u_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n \quad (i = 1, 2, \cdots, n) \tag{27}$$

gedacht wird, so liefert die Vergleichung der Formeln (23) und (26) die unter derselben Voraussetzung bestehende Beziehung:

$$U = V, \tag{28}$$

die auch dahin ausgesprochen werden kann, daß die Form U durch die Substitution (27) in die Form V übergeht. Zwei Formen, für welche dieser Umstand statthat, werden äquivalent genannt. Demnach sind alle zerlegbaren Einheitsformen, auf welche die verschiedenen Basen des Ideals $\mathfrak{m}$ führen, einander äquivalent oder Formen derselben Klasse.

Umgekehrt entspringt aber auch jede Form der gedachten Klasse einer bestimmten Basis des Ideals $\mathfrak{m}$. Denn, ist V irgend eine mit U äquivalente Form, in welche diese durch eine Substitution

(29) $$u_i = a_{1i}v_1 + a_{2i}v_2 + \cdots + a_{ni}v_n \quad (i = 1, 2, \cdots, n)$$

mit der Determinante 1 übergeht, so werden die Zahlen

$$\beta_i = a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n \quad (i = 1, 2, \cdots, n)$$

eine andere Basis des Ideals $\mathfrak{m}$ vorstellen, welcher offenbar die Form V als die aus ihr hervorgehende Einheitsform zugehört.

Allgemeiner gehört dieser Formenklasse die Gesamtheit der zerlegbaren Einheitsformen an, welche allen mit $\mathfrak{m}$ äquivalenten Idealen entspringen. Ist nämlich $\mathfrak{m}' = \beta \cdot \mathfrak{m}$ ein solches Ideal, β also eine ganze oder gebrochene Zahl des Körpers, deren Norm positiv ist, so bilden die Produkte

$$\beta\alpha_1, \ \beta\alpha_2, \ \cdots, \ \beta\alpha_n,$$

welche als in $\mathfrak{m}'$ enthalten ganze Zahlen sein müssen, eine Basis des Ideals $\mathfrak{m}'$. Sind nun die ganzzahligen Werte der Unbestimmten u_i so gewählt, daß F die Zahl α des Ideals $\mathfrak{m}$ vorstellt, so ergeben die Gleichungen (12) die folgenden:

$$\beta\alpha \cdot \omega_i = U_{i1} \cdot \beta\alpha_1 + U_{i2} \cdot \beta\alpha_2 + \cdots + U_{in} \cdot \beta\alpha_n, \quad (i = 1, 2, \cdots, n)$$

in denen $\omega_1, \omega_2, \cdots, \omega_n$ eine Basis von $\mathfrak{g}$ bedeuten, während an Stelle der Gleichungen (14) andere treten von der Form:

$$\beta\alpha_i = g'_{i1}\omega_1 + g'_{i2}\omega_2 + \cdots + g'_{in}\omega_n, \quad (i = 1, 2, \cdots, n)$$

in denen die g'_{ik} ganze rationale Zahlen sind. Daraus fließt statt der Gleichungen (12*) das folgende System

$$\beta\alpha \cdot \omega_i = \sum_{k,\,h} U_{ik} \cdot g'_{kh} \cdot \omega_h, \quad (i = 1, 2, \cdots, n)$$

aus welchem für $N(\beta\alpha)$ der Wert

$$N(\beta\alpha) = |U_{ik}| \cdot |g'_{kh}| = \mathfrak{N}(\beta\mathfrak{m}) \cdot U = \mathfrak{N}(\mathfrak{m}') \cdot U$$

gefunden wird. Man erkennt hieraus, daß allen mit $\mathfrak{m}$ äquivalenten Idealen ein- und dieselbe zerlegbare Einheitsform U, bezw. eine ihr äquivalente Form zugehört. Die gedachte

Formenklasse darf hiernach als die der Idealklasse korrespondierende bezeichnet und gesagt werden:

Jeder Idealklasse korrespondiert eine eindeutig bestimmte Formenklasse zerlegbarer Einheitsformen des Körpers mit der Diskriminante D. Der Transformation der Formen dieser Klasse entspricht der Übergang von einer Basis eines dieser Ideale zu einer andern, und umgekehrt.

Zu den Transformationen der gedachten Formen in einander gehören insbesondere diejenigen der Form U in sich selbst. Wenn die Gleichungen (29) eine solche vorstellen, so ist V die nämliche Form wie U und somit

$$(30)\qquad N(\beta_1 u_1+\beta_2 u_2+\cdots+\beta_n u_n)=N(\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n).$$

Für jedes ganzzahlige Wertsystem der Unbestimmten u_i ist aber

$$F=\alpha_1 u_1+\alpha_2 u_2+\cdots+\alpha_n u_n \text{ eine Zahl } \alpha,$$
$$\Phi=\beta_1 u_1+\beta_2 u_2+\cdots+\beta_n u_n \text{ eine Zahl } \beta$$

in $\mathfrak{m}$ und muß daher

$$N(\beta)=N(\alpha),$$

d. h. $\beta=\varepsilon\alpha$ sein, wo ε eine Zahl des Körpers mit der Norm 1 bedeutet. So ergeben sich insbesondere die Beziehungen

$$(31)\qquad \beta_1=\varepsilon_1\alpha_1,\quad \beta_2=\varepsilon_2\alpha_2,\ \cdots,\ \beta_n=\varepsilon_n\alpha_n,$$

wo die ε_i besondere Zahlen des Körpers mit der Norm 1 bedeuten von der Beschaffenheit, daß diese n Zahlen (31) eine Basis von $\mathfrak{m}$ ausmachen. Alle Transformationen von U in sich selbst befinden sich also jedenfalls unter den Transformationen die dem Übergange von der Basis $\alpha_1, \alpha_2, \cdots, \alpha_n$ zu den verschiedenen Basen von der Art (31) entsprechen. Da für jede Einheit ε mit positiver Norm die Zahlen

$$(32)\qquad \beta_1=\varepsilon\alpha_1,\ \beta_2=\varepsilon\alpha_2,\ \cdots,\ \beta_n=\varepsilon\alpha_n$$

eine Basis der angegebenen Art bilden und zugleich die Gleichung (30) erfüllen, so gibt es, entsprechend allen verschiedenen Einheiten ε unendlich viel Transformationen von U in sich selbst; ob es aber außer den so bestimmten noch andere gibt, die anderen Basen der Art (31) entsprechen, und ob

jeder der letzteren solche Transformationen zukommen, mag hier unerörtert bleiben.

Dagegen ist noch die Frage zu beantworten, ob auch umgekehrt jeder Klasse zerlegbarer Einheitsformen des Körpers mit der Diskriminante D eine *eindeutig* bestimmte oder etwa eine *Mehrheit* verschiedener Idealklassen desselben korrespondiert. Daß jeder solchen Einheitsform ein Ideal und daher auch ihrer Klasse eine Idealklasse des Körpers entspricht, wissen wir aus Nr. 2. Bemerkt man aber, daß die mit Bezug auf den einen Linearfaktor U_1 von E dort angestellte Betrachtung mit Bezug auf jeden andern Linearfaktor von E, welcher etwa ebenfalls aus Zahlen desselben Körpers gebildet ist, durchgeführt werden könnte, so sieht man, daß allgemein derselben Einheitsform des Körpers oder ihrer Klasse soviel Idealklassen desselben korrespondieren werden — ob dieselben wirklich voneinander verschieden sind oder nicht, wäre genauer zu untersuchen — als unter den konjugierten Körpern mit dem gegebenen identische vorhanden sind.

5. Geht so der Äquivalenz der Ideale eines Körpers diejenige der ihm zugehörigen zerlegbaren Formen parallel, so entspricht der Multiplikation der Ideale und der Zusammensetzung ihrer Klassen die Zusammensetzung der Formen resp. ihrer Klassen. Um dies noch kurz zu zeigen, seien

$$(33) \qquad \mathfrak{a} = [\alpha_1, \alpha_2, \cdots, \alpha_n], \; \mathfrak{b} = [\beta_1, \beta_2, \cdots, \beta_n]$$

zwei Ideale des Körpers; ihr Produkt ist wieder ein Ideal $\mathfrak{c}$, welches sowohl durch den Modulus

$$[\cdots, \alpha_i\beta_k, \cdots]$$

mit den n^2 Elementen $\alpha_i\beta_k$ $(i = 1, 2, \cdots, n;\; k = 1, 2, \cdots, n)$, als auch durch einen n-gliedrigen Modulus

$$(34) \qquad \mathfrak{c} = [\gamma_1, \gamma_2, \cdots, \gamma_n]$$

mit den Basiszahlen γ_i darstellbar ist. Daher können einerseits jene durch diese mittels n^2 Gleichungen von der Form

$$(35) \qquad \alpha_i\beta_k = a_1^{(i,k)} \cdot \gamma_1 + a_2^{(i,k)} \cdot \gamma_2 + \cdots + a_n^{(i,k)} \cdot \gamma_n,$$

andererseits diese durch jene mittels n Gleichungen

$$(36)\qquad \gamma_h = c_h^{(1,1)}\cdot\alpha_1\beta_1 + \cdots + c_h^{(i,k)}\cdot\alpha_i\beta_k + \cdots + c_h^{(n,n)}\alpha_n\beta_n,$$
$$(h = 1, 2, \cdots, n)$$

deren Koeffizienten beide Male ganze Zahlen sind, ausgedrückt werden. Setzt man die Ausdrücke (35) in die Gleichungen (36) ein und bedenkt, daß die Basiszahlen γ_i rational unabhängig sind, so ergibt sich folgende Beziehung

$$(37)\qquad \sum_{i,k} a_h^{(i,k)}\; c_{h'}^{(i,k)} = (h, h'),$$

wenn wieder, wie früher, durch das Zeichen (h, h') die Eins oder die Null ausgedrückt wird, je nachdem die beiden der Zahlenreihe $1, 2, \cdots, n$ entnommenen Indices h, h' einander gleich oder verschieden sind. Die in dieser Beziehung auftretende Summe ist aber das Element der Determinante, welche aus den beiden Matrizen der Gleichungen (35), (36) zusammengesetzt und bekanntlich die Summe der Produkte ist, die sich aus den, der ersten Matrix entnommenen n-gliedrigen Determinanten und den entsprechenden der zweiten Matrix bilden lassen. Da der Wert jener Determinante zufolge (37) gleich 1 ist, müssen je die sämtlichen n-gliedrigen Determinanten, die aus den Elementen jeder der Matrizen gebildet werden können, ganze Zahlen ohne gemeinsamen Teiler sein.

Setzt man nunmehr

$$(38)\qquad \begin{aligned} \mathrm{F} &= \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n \\ \Phi &= \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n \\ \Psi &= \gamma_1 w_1 + \gamma_2 w_2 + \cdots + \gamma_n w_n, \end{aligned}$$

so entspringen aus diesen, den Idealen $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ zugehörigen Linearformen drei Einheitsformen U, V, W des Körpers, indem folgende Gleichungen stattfinden:

$$(39)\qquad N(\mathrm{F}) = \mathfrak{N}(\mathfrak{a})\cdot U,\quad N(\Phi) = \mathfrak{N}(\mathfrak{b})\cdot V,\quad N(\Psi) = \mathfrak{N}(\mathfrak{c})\cdot W.$$

Da aus den beiden ersten Gleichungen (38)

$$\mathrm{F}\cdot\Phi = \sum_{i,k} \alpha_i\beta_k\cdot u_i v_k,$$

wegen (35) aber gleich

$$\sum_{i,k,h} a_h^{(i,k)}\cdot u_i v_k\cdot \gamma_h,$$

gefunden wird, so ergibt sich

$$\Psi = \mathrm{F} \cdot \Phi$$

und daher auch

$$N(\Psi) = N(\mathrm{F}) \cdot N(\Phi),$$

wenn

$$w_h = \sum_{i,k} a_h^{(i,k)} \cdot u_i v_k \qquad (40)$$

$$(h = 1, 2, \cdots, n)$$

gesetzt wird; da aber zugleich

$$\mathfrak{N}(\mathfrak{c}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b})$$

ist, so geht die Beziehung

$$W = U \cdot V \qquad (41)$$

hervor, sobald zwischen den Variabeln der drei Formen U, V, W die Gleichungen (40) vorausgesetzt werden. Die Form W, welche dem Idealprodukte $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ entspringt, geht also durch die bilineare Substitution (40), deren Matrix die oben angegebene Eigenschaft hat, in das Produkt der beiden, den Idealen $\mathfrak{a}$, $\mathfrak{b}$ entspringenden Formen U, V über, und wird deshalb die aus den letzteren zusammengesetzte Form genannt.

Es ist bemerkenswert, daß die drei in solcher Weise verbundenen Formen U, V, W unzweideutig durch die bilineare Substitution (40) bestimmt sind. Da nämlich dieser Substitution zufolge

$$\Psi = \mathrm{F} \cdot \Phi$$

ist, findet sich die Beziehung

$$\mathrm{F} \cdot \frac{\partial \Phi}{\partial v_i} = \frac{\partial \Psi}{\partial v_i}$$

d. h.

$$\mathrm{F} \cdot \beta_i = \sum_h \frac{\partial w_h}{\partial v_i} \gamma_h;$$

$$(i = 1, 2, \cdots, n)$$

die in $\mathfrak{c}$ also auch in $\mathfrak{b}$ enthaltenen Zahlen γ_h lassen sich aber als ganzzahlige lineare Ausdrücke von der Form

$$\gamma_h = b_{h1}\beta_1 + b_{h2}\beta_2 + \cdots + b_{hn}\beta_n$$

$$(h = 1, 2, \cdots, n)$$

darstellen, deren Determinante

$$(42) \qquad |b_{i,k}| = (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{g}\mathfrak{b}, \mathfrak{a}\mathfrak{b}) = (\mathfrak{g}, \mathfrak{a}) = \mathfrak{N}(\mathfrak{a})$$

ist, und somit erhält man

$$\mathrm{F} \cdot \beta_i = \sum_{h,k} \frac{\partial w_h}{\partial v_i} b_{hk} \cdot \beta_k,$$

Gleichungen, aus denen man nach Kap. 1, Nr. 8

$$N(\mathrm{F}) = \left| \frac{\partial w_h}{\partial v_i} \right| \cdot |b_{h,k}|$$

d. i. wegen (42) und (39)

$$(43) \qquad U = \left| \frac{\partial w_h}{\partial v_i} \right|$$

erschließt. Auf ganz entsprechende Weise findet sich

$$(44) \qquad V = \left| \frac{\partial w_h}{\partial u_i} \right|$$

und daraus dann W als das Produkt dieser beiden Ausdrücke:

$$(45) \qquad W = \left| \frac{\partial w_h}{\partial u_i} \right| \cdot \left| \frac{\partial w_h}{\partial v_i} \right|.$$

Man überzeugt sich schließlich unschwer, daß, wie die Form W als aus den Formen U, V, so auch ihre Klasse aus den Klassen von U und V zusammengesetzt angesehen werden darf, indem Systeme resp. äquivalenter Formen U und V durch die angegebene Zusammensetzung stets zu äquivalenten Formen W hinführen müssen.

6. Die bisher betrachteten zerlegbaren Formen sind nicht die einzigen, welche dem bestimmten Körper $\mathfrak{K}$ n^{ten} Grades zugehören, wie denn schon aus Nr. 2 hervorgeht, daß er auch solche enthalten kann, deren Diskriminante seiner Grundzahl nicht gleich, sondern in quadratischem Verhältnisse größer ist als sie. In Wahrheit entspricht, wie wir nun nachweisen wollen, jeder besonderen Ordnung des Körpers eine besondere Kategorie von zerlegbaren Formen.

Sei $\mathfrak{o}$ eine bestimmte Ordnung ganzer Zahlen des Körpers und der Modulus

$$(46) \qquad \mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n]$$

ein Ideal in $\mathfrak{o}$, während $\omega_1, \omega_2, \cdots, \omega_n$ eine Basis von $\mathfrak{o}$ bezeichnen. Dann ist die in Nr. 2 mit $\mathfrak{o}$ bezeichnete Ordnung des Modulus $\mathfrak{m}$ mit der hier so benannten Ordnung identisch, die Determinante $|g_{ik}|$ der Gleichungen (14), welche positiv gedacht werden darf, wird, da $\mathfrak{m} \succ \mathfrak{o}$ also $(\mathfrak{m}, \mathfrak{o}) = 1$ ist, mit der Anzahl der (mod. $\mathfrak{m}$) inkongruenten Zahlen der Ordnung, nämlich mit

$$(\mathfrak{o}, \mathfrak{m}) = \mathfrak{N}'(\mathfrak{m}) = \mathfrak{N}(\mathfrak{g}\mathfrak{m})$$

gleich, und statt der Gleichung (16) erhalten wir die Beziehung

$$N(\mathrm{F}) = \mathfrak{N}(\mathfrak{g}\mathfrak{m}) \cdot U, \tag{47}$$

worin U eine ganzzahlige zerlegbare Form n^{ten} Grades mit den n Unbestimmten u_i bedeutet. Da mit Rücksicht auf (14)

$$\Delta(N(\mathrm{F})) = \Delta(\mathfrak{m}) = |g_{ik}|^2 \cdot \Delta(\mathfrak{o}),$$

andererseits nach (7) und (16)

$$\Delta(N(\mathrm{F})) = |g_{ik}|^2 \cdot \Delta(U)$$

gefunden wird, so ergibt sich die Beziehung

$$\Delta(U) = \Delta(\mathfrak{o}) = \mathfrak{N}(\mathfrak{o})^2 \cdot \mathrm{D}, \tag{48}$$

unter $\mathrm{D} = \Delta(\mathfrak{g})$ wieder die Grundzahl des Körpers verstanden.

Jedem Ideale in $\mathfrak{o}$ entspringt also eine zerlegbare Form des Körpers, deren Diskriminante gleich $\mathfrak{N}(\mathfrak{o})^2 \cdot \mathrm{D}$ ist. Diese Form ist wieder eine Einheitsform.

Um den letztern Punkt zu erweisen, bedienen wir uns eines von Dedekind gegebenen Satzes[1]) über Ideale in $\mathfrak{o}$, der dem Satze in Kap. 6, Nr. 17 analog ist und dessen Herleitung wir bis auf diese Stelle verschoben. Er besagt:

Zu jedem Ideale $\mathfrak{a}$ in $\mathfrak{o}$ gibt es ein zweites Ideal $\mathfrak{b}$ der Ordnung, welches mit $\mathfrak{a}$ zusammengesetzt ein Hauptideal der Ordnung hervorbringt, während, wenn $\mathfrak{n}$ einen gegebenen, in $\mathfrak{o}$ enthaltenen Modulus bedeutet, welcher die Gleichung

$$\mathfrak{o}\mathfrak{n} = \mathfrak{n}$$

erfüllt,

$$\mathfrak{b} + \mathfrak{n} = \mathfrak{o}$$

1) S. Festschrift zur Säkularfeier des Geburtstages von C. F. Gauss, Braunschweig 1877, S. 28.

ist. Zum Beweise bemerke man zunächst, daß offenbar $\mathfrak{g}\mathfrak{n}$ ein Körperideal ist. Man setze daher $\mathfrak{g}\mathfrak{n} = \mathfrak{n}' \cdot \mathfrak{f}'$, indem man unter $\mathfrak{f}'$ denjenigen Idealfaktor von $\mathfrak{g}\mathfrak{n}$ versteht, dessen Primideale auch im Führer $\mathfrak{f}$ der Ordnung aufgehen, während das Ideal $\mathfrak{n}'$ aus nicht in $\mathfrak{f}$ aufgehenden Primidealen besteht. Dann gibt es dem zitierten Satze gemäß ein Körperideal $\mathfrak{c}$, welches zu $\mathfrak{n}'$ relativ prim ist und mit dem Körperideale $\mathfrak{g}\mathfrak{a}$ zusammengesetzt ein Ideal $\mathfrak{g}\gamma$ erzeugt, sodaß $\mathfrak{g}\mathfrak{a} \cdot \mathfrak{c}$ oder $\mathfrak{a}\mathfrak{c}$ gleich $\mathfrak{g}\gamma$ gesetzt werden kann, während wegen $\mathfrak{c} + \mathfrak{n}' = \mathfrak{g}$ sich durch Multiplikation mit $\mathfrak{g}\mathfrak{a}$ die Gleichung

$$\mathfrak{g}\gamma + \mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}' = \mathfrak{g}\mathfrak{a} \tag{49}$$

herausstellt. Da sowohl $\mathfrak{g}\mathfrak{a}$ als $\mathfrak{n}'$ und daher auch $\mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}'$ prim gegen $\mathfrak{f}\mathfrak{f}'$, also

$$\mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}' + \mathfrak{f}\mathfrak{f}' = \mathfrak{g}$$

ist, so gibt es ganze Zahlen μ des Körpers, welche die beiden Kongruenzen

$$\mu \equiv \gamma \pmod{\mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}'}, \quad \mu \equiv 1 \pmod{\mathfrak{f}\mathfrak{f}'} \tag{50}$$

erfüllen; sie bilden eine bestimmte Klasse nach dem Modulus $\mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}' - \mathfrak{f}\mathfrak{f}'$ kongruenter Zahlen und folglich kann unter ihnen μ so gewählt werden, daß $N(\mu)$ positiv wird (Kap. 9, Nr. 3). Nach der zweiten der Kongruenzen (50) ist zudem diese Zahl μ kongruent 1 (mod. $\mathfrak{f}$), und da diese Kongruenz (mod. $\mathfrak{f}$) auch (mod. $\mathfrak{o}$) besteht, so ist μ mit 1 zugleich eine Zahl in $\mathfrak{o}$. Demnach ist (s. Kap. 9, Nr. 10) $\mathfrak{o}\mu$ ein Hauptideal der Ordnung. Die erste der Kongruenzen (50) lehrt aber mit Rücksicht auf (49), daß auch

$$\mathfrak{g}\mu + \mathfrak{g}\mathfrak{a} \cdot \mathfrak{n}' = \mathfrak{g}\mathfrak{a} \tag{51}$$

d. h. $\mathfrak{g}\mu \succ \mathfrak{g}\mathfrak{a}$ und folglich

$$\mathfrak{g}\mu = \mathfrak{g}\mathfrak{a} \cdot \mathfrak{d} \tag{52}$$

ist, wo $\mathfrak{d}$ ein Körperideal bedeutet, welches ebenso wie $\mathfrak{g}\mu$ zu $\mathfrak{f}$ prim ist; daher gibt es ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$, für welches $\mathfrak{g}\mathfrak{b} = \mathfrak{d}$ und wegen (52)

$$\mathfrak{g} \cdot \mathfrak{o}\mu = \mathfrak{g}\mathfrak{a} \cdot \mathfrak{g}\mathfrak{b} = \mathfrak{g} \cdot \mathfrak{a}\mathfrak{b} \tag{53}$$

ist. Hieraus folgt einerseits (nach Kap. 9, Nr. 2)

$$\mathfrak{o}\mu = \mathfrak{a}\mathfrak{b}, \tag{54}$$

andererseits aus (51)

$$\mathfrak{g}\cdot\mathfrak{a}\mathfrak{b} + \mathfrak{g}\cdot\mathfrak{a}\mathfrak{n}' = \mathfrak{g}\mathfrak{a}$$

d. i.

$$\mathfrak{g}\mathfrak{a}(\mathfrak{g}\mathfrak{b} + \mathfrak{n}') = \mathfrak{g}\mathfrak{a}\cdot\mathfrak{g},$$

aus welcher Gleichung zwischen Körperidealen

$$\mathfrak{g}\mathfrak{b} + \mathfrak{n}' = \mathfrak{g}$$

hervorgeht. Diese Gleichung lehrt, daß $\mathfrak{g}\mathfrak{b}$ prim ist gegen $\mathfrak{n}'$, und da es nach (53) mit μ zugleich prim ist gegen $\mathfrak{f}\mathfrak{f}'$, so ist es prim auch gegen $\mathfrak{f}\mathfrak{f}'\cdot\mathfrak{n}' = \mathfrak{g}\mathfrak{n}\mathfrak{f}$, in Zeichen

$$\mathfrak{g}\mathfrak{b} + \mathfrak{g}\mathfrak{n}\mathfrak{f} = \mathfrak{g}$$

oder

$$\mathfrak{g}(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) = \mathfrak{g}\cdot\mathfrak{o}. \tag{55}$$

Nun ist $\mathfrak{b} + \mathfrak{n}\mathfrak{f}$ ein Ideal in $\mathfrak{o}$, denn nach der von $\mathfrak{n}$ vorausgesetzten Eigenschaft ist

$$\mathfrak{o}(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) = \mathfrak{b} + \mathfrak{n}\mathfrak{f},$$

während

$$(\mathfrak{b} + \mathfrak{n}\mathfrak{f}) + \mathfrak{f} = \mathfrak{o} + \mathfrak{n}\mathfrak{f} = \mathfrak{o}$$

ist. Somit folgt aus (55) nach Kap. 9, Nr. 2 die Gleichung $\mathfrak{b} + \mathfrak{n}\mathfrak{f} = \mathfrak{o}$, und da $\mathfrak{n}\mathfrak{f} \succ \mathfrak{n}\mathfrak{o} = \mathfrak{n}$ ist, offenbar auch die verlangte Beziehung

$$\mathfrak{b} + \mathfrak{n} = \mathfrak{o}. \tag{56}$$

Mit den Gleichungen (54) und (56) ist die Behauptung des Satzes bewiesen.

Nunmehr sei k irgend eine rationale ganze Zahl. Dann ist $\mathfrak{o}k$ ein Modulus, wie der Modulus $\mathfrak{n}$ des Satzes, und es gibt, wenn wir zum Ideale $\mathfrak{a} = \mathfrak{m}$ und der Formel (47) zurückkehren, dem Hilfssatze gemäß ein Ideal $\mathfrak{b}$ der Ordnung, für welches $\mathfrak{m}\cdot\mathfrak{b}$ ein Hauptideal $\mathfrak{o}\mu$ in $\mathfrak{o}$ und $\mathfrak{b} + \mathfrak{o}k = \mathfrak{o}$ mithin $\mathfrak{g}\mathfrak{b} + \mathfrak{g}k = \mathfrak{g}$, d. h. das Ideal $\mathfrak{g}\mathfrak{b}$ prim ist gegen k; nach Kap. 6, Nr. 18 ist daher auch $\mathfrak{N}(\mathfrak{g}\mathfrak{b})$ prim gegen k. Die Gleichung (51), welche für die Zahl μ stattfand, zeigt, daß $\mathfrak{g}\mu$ und somit die in $\mathfrak{o}$ enthaltene Zahl μ auch in $\mathfrak{g}\mathfrak{m}$ also in $\mathfrak{o} - \mathfrak{g}\mathfrak{m} = \mathfrak{m}$ enthalten ist. Wählt man daher für die Unbestimmten u_i die-

jenigen Werte, durch welche F in μ übergeht, so folgt einerseits mit Rücksicht auf

$$\mathfrak{o}\mu = \mathfrak{m} \cdot \mathfrak{b} \quad \text{also} \quad \mathfrak{g}\mu = \mathfrak{g}\mathfrak{m} \cdot \mathfrak{g}\mathfrak{b}$$

die Gleichung

$$N(\mu) = \pm\, \mathfrak{N}(\mathfrak{g}\mu) = \pm\, \mathfrak{N}(\mathfrak{g}\mathfrak{m}) \cdot \mathfrak{N}(\mathfrak{g}\mathfrak{b}),$$

andererseits wegen (47)

$$N(\mu) = \mathfrak{N}(\mathfrak{g}\mathfrak{m}) \cdot U$$

also

$$U = \pm\, \mathfrak{N}(\mathfrak{g}\mathfrak{b})$$

d. h. relativ prim zu jeder beliebigen Zahl k, was nur sein kann, wenn U eine Einheitsform ist.

Nachdem so der obige Satz vollständig bewiesen worden ist, übersieht man sogleich, daß, was von der Äquivalenz und über die Zusammensetzung der Formen und ihrer Klassen, welche den Körperidealen entsprangen, gezeigt worden ist, sich kraft der Definition der Äquivalenz für Ideale in $\mathfrak{o}$ unmittelbar in gleicher Weise auch für die Ideale der Ordnung aussagen läßt: jeder Idealklasse korrespondiert eine eindeutig bestimmte Formenklasse, und der Multiplikation der Ideale die Zusammensetzung der entsprechenden Formen.

Wenn es daher unnötig scheint, hierauf näher einzugehen, so muß dagegen noch bemerkt werden, daß die Gesamtheit der möglichen zerlegbaren Formen n^{ten} Grades des Körpers auch mit der Betrachtung dieser den Idealen jeder Ordnung entsprechenden Formen noch nicht erschöpft zu sein braucht. Denn der aus ganzen Zahlen des Körpers bestehende Modulus $\mathfrak{m}$, den wir durch die Formel (11) ausgedrückt haben, braucht im allgemeinen weder ein Körperideal noch ein Ideal irgend einer Ordnung zu sein, und doch führt die in Nr. 2 angestellte Betrachtung durch die dortige Formel (16) zu einer dem Modulus entsprechenden zerlegbaren Form, die dem Körper zugehören kann. Da aus (14) und (16) wieder einerseits

$$\Delta(N(\mathrm{F})) = \Delta(\mathfrak{m}) = |\, g_{ik} \,|^2 \cdot \Delta(\mathfrak{o}),$$

andererseits

$$\Delta(N(\mathrm{F})) = |\, g_{ik} \,|^2 \cdot \Delta(U)$$

sich ergibt, so erschließt man für die Diskriminante der gedachten Form U wieder den Wert

$$\Delta(U) = \Delta(\mathfrak{o}) = \mathfrak{N}(\mathfrak{o})^2 \cdot \mathrm{D}, \tag{57}$$

wo $\mathfrak{o}$ die Bedeutung der Nr. 2 hat. Auch hier gelten dann über die Äquivalenz der den verschiedenen Moduln entsprechenden Formen U analoge Sätze, wie in den vorigen Fällen. Man kann nämlich auch für ganzzahlige Moduln die Äquivalenz in gleicher Weise definieren, wie für Ideale, so daß zwei n-gliedrige Moduln $\mathfrak{m}$, $\mathfrak{m}'$ des Körpers einander äquivalent heißen sollen, wenn eine Zahl β mit positiver Norm vorhanden ist, für welche $\mathfrak{m}' = \beta \cdot \mathfrak{m}$ ist; hiernach lassen sich dann sämtliche jener Moduln in Klassen äquivalenter Moduln verteilen. Alle Moduln $\mathfrak{m}$ derselben Klasse aber haben gleiche Quotienten $\mathfrak{m}^0$ oder dieselbe Ordnung, denn, wenn μ irgend eine Zahl in $\mathfrak{m}^0$ und folglich $\mu\mathfrak{m} \succ \mathfrak{m}$ ist, so ergibt sich durch Multiplikation mit β daraus $\mu\mathfrak{m}' \succ \mathfrak{m}'$, d. h. μ gehört auch zu $(\mathfrak{m}')^0$, und ebenso auch umgekehrt. Durchläuft nun $\mathfrak{a}$ alle Moduln einer Klasse A, $\mathfrak{b}$ alle diejenigen einer Klasse B, so werden die Produkte $\mathfrak{a}\mathfrak{b}$ wieder einer ganz bestimmten Klasse C angehörig sein, welche, wie bei den Idealen, die aus A, B zusammengesetzte Klasse heißt, und man sieht demnach, daß für die Äquivalenz und Zusammensetzung der den Moduln entspringenden zerlegbaren Formen U sich Sätze herausstellen müssen, welche den früheren völlig analog sind.

Im Zusamenhange hiermit bemerken wir die in Nr. 2 gefundene Beziehung

$$\Delta(\mathfrak{m}) = |a_{ik}|^2 \cdot \mathfrak{N}(\mathfrak{a})^2 \cdot \mathrm{D}$$

oder

$$\mathrm{D} \cdot |a_{ik}|^2 = \frac{\Delta(\mathfrak{m})}{\mathfrak{N}(\mathfrak{a})^2}. \tag{58}$$

Dieser Quotient ist nicht nur dem bestimmten Modulus $\mathfrak{m}$ eigentümlich, sondern eine Invariante der ganzen Klasse, der er angehört. In der Tat, geht man von dem Modulus

$$\mathfrak{m} = [\alpha_1, \alpha_2, \cdots, \alpha_n],$$

welchem das Ideal (s. Nr. 2)

$$\mathfrak{a} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\} = [\beta_1, \beta_2, \cdots, \beta_n]$$

entsprach, zu dem äquivalenten Modulus $\mathfrak{m}' = \beta\mathfrak{m}$ über, dessen

ganzzahlige Basiszahlen $\beta\alpha_1, \beta\alpha_2, \cdots, \beta\alpha_n$ sein werden, und welchem das mit $\mathfrak{a}$ äquivalente Ideal

$$\mathfrak{a}' = \beta\mathfrak{a} = \{\beta\alpha_1, \beta\alpha_2, \cdots, \beta\alpha_n\}$$

entspricht, so werden offenbar $\beta\beta_1, \beta\beta_2, \cdots, \beta\beta_n$ eine ganzzahlige Basis des letztern sein; zwischen den Basiszahlen von $\mathfrak{m}'$ einerseits und denen von $\mathfrak{a}'$ andererseits bestehen daher die gleichen Beziehungen (18), wie zwischen denen von $\mathfrak{m}$ und denen von $\mathfrak{a}$, die linke Seite der Formel (58) bleibt daher ungeändert, und demnach ist, wie behauptet:

$$\frac{\Delta(\mathfrak{m}')}{\mathfrak{N}(\mathfrak{a}')^2} = \frac{\Delta(\mathfrak{m})}{\mathfrak{N}(\mathfrak{a})^2}.$$

Man bezeichnet daher den Quotienten

$$\frac{\Delta(\mathfrak{m})}{\mathfrak{N}(\mathfrak{a})^2}$$

als die Diskriminante der Modulklasse von $\mathfrak{m}$.

Wir fügen endlich noch die Beziehung an:

$$\frac{(\mathfrak{o}, \mathfrak{m})}{(\mathfrak{m}, \mathfrak{o})} = \sqrt{\frac{\Delta(\mathfrak{m})}{\Delta(\mathfrak{o})}},$$

welche aus der Gleichung (57) durch Vergleichung mit (15) sich ergibt; sie ist nur ein spezieller Fall der für irgend zwei Moduln (11) geltenden, von Dedekind gegebenen Formel[1]):

$$\frac{(\mathfrak{m}', \mathfrak{m})}{(\mathfrak{m}, \mathfrak{m}')} = \sqrt{\frac{\Delta(\mathfrak{m})}{\Delta(\mathfrak{m}')}}.$$

Elftes Kapitel.

Unterkörper und Oberkörper.

1. Haben wir bisher meist einen einzelnen Zahlenkörper für sich betrachtet, so müssen wir nun noch die Aufmerksamkeit auf die Beziehungen lenken, welche zwischen zwei ver-

1) Dirichlets Vorlesungen über Zahlentheorie, herausg. von Dedekind, 4. Auflage, p. 537.

schiedenen Körpern bestehen. Algebraisch äußern sich dieselben in der sogenannten Verwandtschaft der algebraischen Gleichungen, d. i. in der Art des Zusammenhanges, der zwischen den die Körper erzeugenden Zahlen oder den Gleichungen, durch welche diese bestimmt werden, vorhanden sein kann, und es sind da namentlich die Beziehungen, welche einen Körper mit seinen Unterkörpern verbinden, die für die Eigenschaften der algebraischen Gleichungen und die Gesetze ihrer Auflösung von Wichtigkeit sind. Hier, wo wir es nur mit den arithmetischen Eigenschaften der Zahlenkörper zu tun haben, wird es hauptsächlich interessieren, wie die Idealtheorien, die für jeden der Körper besonders gelten, sich zu einander verhalten, in einander greifen, bezw. auf einander zurückführbar sind, wie insbesondere die Zerlegung der rationalen Primzahlen in Primideale, welche für einen Körper gilt, sich zu derjenigen im andern verhält, nach welchen Gesetzen die Primfaktoren der Diskriminante des einen mit denen des andern übereinstimmen u. dgl. m.

Indem wir hierüber in diesem und dem folgenden Kapitel noch einige wichtige Ergebnisse aussagen wollen, richten wir vor allem unsern Blick auf den Begriff des Ideales. Sei $\mathfrak{K}$ ein gegebener Körper N^{ten} Grades und $\mathfrak{k}$ irgend ein Unterkörper, d. h. ein in ihm enthaltener Körper, dessen Grad n heiße. In diesem Körper sei

$$\mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_h\}$$

irgend ein Ideal, der Definition eines solchen zufolge also die Gesamtheit der Zahlen von der Form

$$\gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_h\alpha_h,$$

in der die Koeffizienten γ_i alle ganzen Zahlen in $\mathfrak{k}$ bedeuten. Da die Zahlen α_i auch dem Körper $\mathfrak{K}$ angehören, so bildet die Gesamtheit der Zahlen von der Form

$$\Gamma_1\alpha_1 + \Gamma_2\alpha_2 + \cdots + \Gamma_h\alpha_h,$$

in welcher die Koeffizienten Γ_i alle ganzen Zahlen in $\mathfrak{K}$ bedeuten, und die wir durch

$$\mathfrak{J} = \{\alpha_1, \alpha_2, \cdots, \alpha_h\}'$$

bezeichnen wollen, ein Ideal des Körpers $\mathfrak{K}$. Demnach ent-

spricht jedem Ideale $\mathfrak{j}$ des Unterkörpers ein Ideal $\mathfrak{J}$ des Oberkörpers, das jenes in sich enthält und ihm als gleich oder gleichbedeutend angesehen werden darf. Heißt $\mathfrak{G}$ die Gesamtheit aller ganzen Zahlen in $\mathfrak{K}$, so besteht offenbar zwischen den beiden Idealen $\mathfrak{j}$ und $\mathfrak{J}$ die Beziehung

$$\mathfrak{J} = \mathfrak{G}\mathfrak{j}.$$

Das Umgekehrte gilt nicht in gleicher Weise. Ist nämlich

$$J = \{A_1, A_2, \cdots, A_H\}'$$

ein Ideal des Körpers $\mathfrak{K}$, so werden zwar die Zahlen, welche diesem Ideale und dem Unterkörper $\mathfrak{k}$ gemeinsam sind, ein Ideal $\mathfrak{j}$ des letzteren bilden, da einerseits Summe und Differenz zweier solcher Zahlen, andererseits auch jedes Produkt einer solchen Zahl in eine Zahl des Körpers $\mathfrak{k}$ sowohl zu J als auch zu $\mathfrak{k}$ und demnach wieder der Gesamtheit der gedachten Zahlen angehört. Ist aber etwa

$$\mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_h\}$$

also

$$\mathfrak{J} = \{\alpha_1, \alpha_2, \cdots, \alpha_h\}' = \mathfrak{G}\mathfrak{j}$$

das ihm gleichbedeutende Ideal des Körpers $\mathfrak{K}$, so kann J nur dann als ein Ideal in $\mathfrak{k}$ angesehen werden, wenn $J = \mathfrak{J}$, d. h. wenn es in $\mathfrak{j}$ Zahlen $\alpha_1, \alpha_2, \cdots, \alpha_h$ gibt, deren größtem gemeinsamen Idealteiler

$$\Gamma_1\alpha_1 + \Gamma_2\alpha_2 + \cdots + \Gamma_h\alpha_h$$

in $\mathfrak{K}$ das Ideal J gleich ist.

Ferner bemerken wir, daß die Gesamtheit der Zahlen

$$\mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_h\} = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_h\alpha_h$$

beim Übergange vom Körper $\mathfrak{k}$ zu einem seiner konjugierten $\mathfrak{k}^{(i)}$ in die Gesamtheit der Zahlen

$$\gamma_1^{(i)}\alpha_1^{(i)} + \gamma_2^{(i)}\alpha_2^{(i)} + \cdots + \gamma_h^{(i)}\alpha_h^{(i)}$$

verwandelt wird, wo die Koeffizienten $\gamma_k^{(i)}$ sämtliche ganze Zahlen des konjugierten Körpers bedeuten; es verwandelt sich mit anderen Worten jedes Ideal $\mathfrak{j}$ in $\mathfrak{k}$ in ein konjugiertes Ideal $\mathfrak{j}^{(i)}$ in $\mathfrak{k}^{(i)}$. Man sieht zugleich, daß die zu einem *Prim*ideale $\mathfrak{p}$ konjugierten Ideale $\mathfrak{p}^{(i)}$ eben-

falls *Prim*ideale sind; denn, wäre $\mathfrak{p}^{(i)} = \mathfrak{q}^{(i)} \cdot \mathfrak{r}^{(i)}$, so fände sich beim Rückgange zum Körper $\mathfrak{k}$ die Gleichung $\mathfrak{p} = \mathfrak{q} \cdot \mathfrak{r}$, wo ein Faktor $\mathfrak{q}$ nur dann gleich der Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen des Körpers $\mathfrak{k}$ sein könnte, wenn $\mathfrak{q}^{(i)} = \mathfrak{g}^{(i)}$ d. i. die Gesamtheit der ganzen Zahlen in $\mathfrak{k}^{(i)}$ wäre, was nicht vorausgesetzt wird.

Nun war, wenn $\alpha_1, \alpha_2, \cdots, \alpha_n$ eine Basis von $\mathfrak{j}$ und

$$\mathrm{F} = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

die Fundamentalform des Ideales ist,

$$N(\mathrm{F}) = \mathfrak{N}(\mathfrak{j}) \cdot E, \tag{1}$$

wo E eine Einheitsform bezeichnet. Dieser Formel zufolge ist $\mathfrak{N}(\mathfrak{j})$ der Inhalt der Form $N(\mathrm{F})$. Denken wir uns aber den Galoisschen Körper K, welcher aus den n konjugierten Körpern $\mathfrak{k}, \mathfrak{k}^{(1)}, \mathfrak{k}^{(2)}, \cdots, \mathfrak{k}^{(n-1)}$ zusammengesetzt ist, also jeden derselben als einen Unterkörper in sich enthält, so sind die konjugierten Ideale $\mathfrak{j}, \mathfrak{j}^{(1)}, \mathfrak{j}^{(2)}, \cdots, \mathfrak{j}^{(n-1)}$ nach dem eben Bemerkten auch als Ideale in K zu betrachten, und nach dem fundamentalen Satze in Kap. 7, Nr. 3 wird der Inhalt der Form $N(\mathrm{F})$ auch durch das Produkt der Inhalte der einzelnen Linearfaktoren dieser Form, d. i. durch das Produkt

$$N(\mathfrak{j}) = \mathfrak{j} \cdot \mathfrak{j}^{(1)} \cdot \mathfrak{j}^{(2)} \cdots \mathfrak{j}^{(n-1)} \tag{2}$$

der konjugierten Ideale bestimmt. Daraus entnehmen wir die allgemeine Gleichheit

$$\mathfrak{N}(\mathfrak{j}) = N(\mathfrak{j}), \tag{3}$$

welche von uns bisher nur für Hauptideale festgestellt worden war. Die durch das Zeichen $\mathfrak{N}(\mathfrak{j})$ ausgedrückte Anzahl der (mod. $\mathfrak{j}$) inkongruenten ganzen Zahlen des Körpers $\mathfrak{k}$ darf mithin stets als die in bezug auf diesen Körper $\mathfrak{k}$ gebildete Norm des Ideales angesehen werden, womit die Wahl des Ausdruckes „Norm" für jene Anzahl gerechtfertigt wird.

2. Der Grad n des Unterkörpers $\mathfrak{k}$ ist nach Kap. 1, Nr. 13 ein Teiler vom Grade N des Oberkörpers $\mathfrak{K}$. Wenn nämlich

$$x^N + A_1 x^{N-1} + A_2 x^{N-2} + \cdots + A_N = 0 \tag{4}$$

die ganzzahlige Gleichung ist, der eine den Körper $\mathfrak{K}$ erzeu-

gende Zahl A, welche als ganze algebraische Zahl vorausgesetzt werden darf, Genüge leistet, desgleichen

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0 \tag{5}$$

die ganzzahlige Gleichung, welche eine den Unterkörper $\mathfrak{k}$ erzeugende ganze Zahl α bestimmt, so reduziert sich die erstere nach Kap. 1, Nr. 10 und 13 durch Adjunktion der Zahl α zu ihrem ursprünglichen Rationalitätsbereiche R auf eine in $\mathfrak{k}$ irreduktible Gleichung

$$x^r + k_1(\alpha) x^{r-1} + k_2(\alpha) x^{r-2} + \cdots + k_r(\alpha) = 0, \tag{6}$$

welche A zur Wurzel hat und deren Koeffizienten dem Unterkörper $\mathfrak{k}$ angehören. Indem man nun den Körper $\mathfrak{K}$ aus der Wurzel A dieser Gleichung, d. h. aus A und α gebildet denkt oder, mit anderen Worten, als den Rationalitätsbereich des Körpers $\mathfrak{K}$ nicht mehr den Bereich R der rationalen Zahlen, sondern den Körper $\mathfrak{k}$ der Betrachtung zugrunde legt, nennt man den Körper $\mathfrak{K}$, der dann nur noch r^{ten} Grades ist, einen mit Bezug auf $\mathfrak{k}$ genommenen Körper oder einen Relativkörper. Die $N = r \cdot n$ Substitutionen, durch welche der Körper $\mathfrak{K} = K(\mathrm{A}; R)$ in seine Konjugierten und die Wurzel A der Gleichung (4) in die übrigen Wurzeln derselben übergeht, und deren eine jede zugleich auch eine Substitution des Unterkörpers $\mathfrak{k}$ bestimmt, zerfallen dann nach Kap. 1, Nr. 10 in n Komplexe von je r Substitutionen, für deren ersten der Körper $\mathfrak{k}$ ungeändert bleibt, A aber in die übrigen Wurzeln der Gleichung (6), für deren übrige $\mathfrak{k}$ in seine Konjugierten $\mathfrak{k}^{(i)}$ und A resp. in die Wurzeln der zu (6) konjugierten Gleichungen

$$x^r + k_1(\alpha^{(i)}) x^{r-1} + k_2(\alpha^{(i)}) x^{r-2} + \cdots + k_r(\alpha^{(i)}) = 0, \tag{7}$$

die hier mit

$$\mathrm{A}_i,\ \mathrm{A}_i^{(1)},\ \mathrm{A}_i^{(2)},\ \ldots,\ \mathrm{A}_i^{(r-1)} \tag{8}$$

bezeichnet werden mögen, übergeht. Die Wurzeln

$$\mathrm{A},\ \mathrm{A}^{(1)},\ \mathrm{A}^{(2)},\ \ldots,\ \mathrm{A}^{(r-1)},$$

welche der Gleichung (6) entsprechen, resp. die aus ihnen erzeugten Körper

$$\mathfrak{K},\ \mathfrak{K}^{(1)},\ \mathfrak{K}^{(2)},\ \ldots,\ \mathfrak{K}^{(r-1)}$$

r^{ten} Grades sollen die zur Zahl A bezw. zum Körper $\mathfrak{K}$

relativ konjugierten Zahlen resp. Körper genannt werden.

Da jede Zahl des Relativkörpers $\mathfrak{K} = K(\mathrm{A};\, \mathfrak{k})$ nach der angezogenen Stelle auf eindeutig bestimmte Weise in die Form

$$(9)\quad Z = c_0(\alpha) + c_1(\alpha)\mathrm{A} + c_2(\alpha)\mathrm{A}^2 + \cdots + c_{r-1}(\alpha)\mathrm{A}^{r-1},$$

in der die Koeffizienten Zahlen in $\mathfrak{k}$ sind, gesetzt werden kann, so entstehen daraus durch die r Substitutionen von $\mathfrak{K}$, welche $\mathfrak{k}$ ungeändert lassen, die zu Z relativ konjugierten Zahlen

$$Z^{(i)} = c_0(\alpha) + c_1(\alpha)\mathrm{A}^{(i)} + c_2(\alpha)\mathrm{A}^{(i)2} + \cdots + c_{r-1}(\alpha)\mathrm{A}^{(i)r-1},$$

deren Produkt die Relativnorm der Zahl Z heißen und durch das Zeichen

$$(10)\qquad N_{\mathfrak{k}}(Z) = Z \cdot Z^{(1)} \ldots Z^{(r-1)}$$

ausgedrückt werden soll. Da sie in bezug auf die Wurzeln der Gleichung (6), deren Koeffizienten ebenso wie diejenigen der Zahl Z dem Körper $\mathfrak{k}$ angehören, symmetrisch ist, so ist sie ebenfalls eine Zahl des Körpers $\mathfrak{k}$.

Ebenso wie jede einzelne Zahl Z des Relativkörpers durch die angegebenen r Substitutionen in die relativ konjugierten Zahlen $Z^{(i)}$, so geht durch sie jedes System solcher Zahlen in ein entsprechendes System, insbesondere, wie nach den Vorbemerkungen in Nr. 1 einleuchtend ist, jedes Ideal des Relativkörpers, d. h. eine Gesamtheit

$$(11)\qquad \mathfrak{J} = \Gamma_1 \mathrm{A}_1 + \Gamma_2 \mathrm{A}_2 + \cdots + \Gamma_H \mathrm{A}_H,$$

in welcher die A_i bestimmte, die Γ_i sämtliche ganze Zahlen des Relativkörpers bedeuten, durch die gedachten Substitutionen in die relativ konjugierten Ideale $\mathfrak{J}^{(i)}$ über. Die Relativnorm des Ideales $\mathfrak{J}$, nämlich das Produkt

$$N_{\mathfrak{k}}(\mathfrak{J}) = \mathfrak{J} \cdot \mathfrak{J}^{(1)} \cdot \mathfrak{J}^{(2)} \ldots \mathfrak{J}^{(r-1)}$$

ist ein Ideal des Körpers $\mathfrak{k}$. In der Tat gestattet offenbar der Fundamentalsatz in Kap. 7, Nr. 3 eine Übertragung von dem Falle, daß der Rationalitätsbereich des Körpers $\mathfrak{K}$ der Bereich R ist, auf den anderen Fall, daß er ein beliebiger Unterkörper $\mathfrak{k}$ von $\mathfrak{K}$ ist, und man findet dementsprechend

$$(12)\qquad N_{\mathfrak{k}}(\mathrm{A}_1 U_1 + \mathrm{A}_2 U_2 + \cdots + \mathrm{A}_H U_H) = N_{\mathfrak{k}}(\mathfrak{J}) \cdot E,$$

wenn unter E eine Form mit den Unbestimmten U_i verstanden wird, deren Koeffizienten Zahlen ohne gemeinsamen Idealteiler in $\mathfrak{K}$, d. i. mit dem größten gemeinsamen Teiler $\mathfrak{G}$ sind. Demnach ist $N_{\mathfrak{k}}(\mathfrak{J})$ der Inhalt der Form zur Linken der Gleichung (12), oder das Ideal, welches durch die offenbar zu $\mathfrak{k}$ gehörigen Koeffizienten dieser Form bestimmt ist.

Unter der Relativdifferente einer Zahl Z des Körpers $\mathfrak{K}$ versteht man den Ausdruck

$$(13)\qquad \partial_{\mathfrak{k}}(Z) = (Z - Z^{(1)})(Z - Z^{(2)}) \cdots (Z - Z^{(r-1)}).$$

Denkt man in ihn die Werte der $Z^{(i)}$ eingesetzt, so hat er die Form einer ganzen Funktion von A, $\mathrm{A}^{(1)}$, $\mathrm{A}^{(2)}, \ldots, \mathrm{A}^{(r-1)}$, welche in bezug auf die letzten $r-1$ dieser Wurzeln der Gleichung (6) symmetrisch ist; er ist also eine ganze Funktion von A allein mit Koeffizienten, welche zu $\mathfrak{k}$ gehören, mithin eine Zahl des Relativkörpers $\mathfrak{K} = K(\mathrm{A};\, \mathfrak{k})$.

Entsprechend heißt Relativdiskriminante von Z der Ausdruck

$$(14)\qquad \Delta_{\mathfrak{k}}(Z) = \begin{vmatrix} 1, & Z, & Z^2, & \ldots, & Z^{r-1} \\ 1, & Z^{(1)}, & Z^{(1)\,2}, & \ldots & Z^{(1)\,r-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & Z^{(r-1)}, & Z^{(r-1)\,2}, & \ldots, & Z^{(r-1)\,r-1} \end{vmatrix}^2$$

oder

$$(14^{\mathrm{a}})\qquad \Delta_{\mathfrak{k}}(Z) = (Z - Z^{(1)})^2 \cdot (Z - Z^{(2)})^2 \cdots (Z^{(r-2)} - Z^{(r-1)})^2,$$

welcher mit dem Ausdrucke (13) durch die Gleichung

$$(15)\qquad \Delta_{\mathfrak{k}}(Z) = (-1)^{\frac{r(r-1)}{2}} \cdot N_{\mathfrak{k}}(\partial_{\mathfrak{k}}(Z))$$

zusammenhängt und demnach (vgl. das zu (10) Bemerkte) sich als eine Zahl in $\mathfrak{k}$ herausstellt.

Bezeichnen nun

$$\Omega_1,\ \Omega_2,\ \cdots,\ \Omega_N$$

die Basiszahlen für die Gesamtheit aller ganzen Zahlen des Körpers $\mathfrak{K}$ N^{ten} Grades und

$$\Omega_1^{(i)},\ \Omega_2^{(i)},\ \cdots,\ \Omega_N^{(i)}$$

diejenigen für die Gesamtheit aller ganzen Zahlen des relativ konjugierten Körpers $\mathfrak{K}^{(i)}$, so bestimmen die Ausdrücke

$$(16)\qquad \mathfrak{E}^{(i)} = \{\Omega_1 - \Omega_1^{(i)}, \Omega_2 - \Omega_2^{(i)}, \cdots, \Omega_N - \Omega_N^{(i)}\}$$
$$(i = 1, 2, \cdots, r-1)$$

$r - 1$ Ideale, welche zwar im allgemeinen nicht dem Körper $\mathfrak{K}$ selbst, sondern erst einem umfassenderen Körper angehörig sind; sie mögen die Elemente des Relativkörpers und ihr Produkt

$$(17)\qquad \mathfrak{D}_{\mathfrak{k}} = \mathfrak{E}^{(1)} \cdot \mathfrak{E}^{(2)} \ldots \mathfrak{E}^{(r-1)}$$

die Relativdifferente des Körpers $\mathfrak{K}$ heißen. Sie ist ein Ideal in $\mathfrak{K}$. In der Tat, bedeutet

$$(18)\qquad W = \Omega_1 U_1 + \Omega_2 U_2 + \cdots + \Omega_N U_N$$

die Fundamentalform des Körpers $\mathfrak{K}$, so ist die Relativdifferente von W, nämlich

$$(19)\qquad \partial_k(W) = (W - W^{(1)})(W - W^{(2)}) \cdots (W - W^{(r-1)})$$

eine Form mit den Unbestimmten U_i und mit Koeffizienten, welche Zahlen in $\mathfrak{K}$ sind, da die von W zugleich mit den Ω_i durch α und die erzeugende Zahl A ausdrückbar sind und dann Ähnliches gilt wie für $\partial_{\mathfrak{k}}(Z)$. Da aber (aus dem verallgemeinerten Fundamentalsatze in Kap. 7, Nr. 3) $\mathfrak{D}_{\mathfrak{k}}$ als der Inhalt dieser Form, d. i. als größter gemeinsamer Idealteiler ihrer Koeffizienten befunden wird, so ist er, wie behauptet, ein Ideal in $\mathfrak{K}$.

Die Determinanten r^{ten} Grades, welche aus der Matrix

$$(20)\qquad \left\| \begin{matrix} \Omega_1, & \Omega_2, & \cdots\cdots, & \Omega_N \\ \Omega_1^{(1)}, & \Omega_2^{(1)}, & \cdots\cdots, & \Omega_N^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \cdots, & \Omega_N^{(r-1)} \end{matrix} \right\|$$

gebildet werden können, sollen kurz die Determinanten der Matrix heißen. Das Quadrat einer jeden solchen Determinante ist offenbar symmetrisch in bezug auf die relativ konjugierten Körper, d. i. auf die Wurzeln der Gleichung (6) und demnach eine Zahl in $\mathfrak{k}$. Nennt man daher Relativdiskriminante des Körpers $\mathfrak{K}$ das Quadrat des größten Idealteilers, welcher jenen Determinanten gemeinsam ist, so ist diese Relativdiskriminante $\mathrm{D}_{\mathfrak{k}}$ ein Ideal des Körpers $\mathfrak{k}$.

3. Zwischen den im Vorhergehenden definierten Größen selbst, sowie zwischen ihnen und den Diskriminanten der Körper $\mathfrak{K}$ und $\mathfrak{k}$ bestehen einige wichtige Beziehungen, die vor allem abgeleitet werden sollen.[1]) Wir erinnern zu diesem Zwecke zunächst an ein schon früher (Kap. 7, Nr. 7) erhaltenes Resultat. Aus (18) folgen Gleichungen von der Form:

$$W^i = U_{1i}\Omega_1 + U_{2i}\Omega_2 + \cdots + U_{Ni}\Omega_N, \tag{21}$$
$$(i = 0, 1, 2, \cdots, N-1)$$

in denen die U_{ik} ganze, ganzzahlige Funktionen der Unbestimmten U_i sind; daher ergibt sich umgekehrt

$$\Omega_i = \frac{V_{i0} + V_{i1}W + V_{i2}W^2 + \cdots + V_{i,N-1}W^{N-1}}{U}, \tag{22}$$
$$(i = 1, 2, \cdots, N)$$

wo die V_{ik} ebenfalls ganze, ganzzahlige Funktionen jener Unbestimmten, und

$$U = |U_{ik}|$$

nach der angezogenen Stelle eine ganzzahlige Einheitsform mit denselben Unbestimmten bezeichnet.

Nun betrachte man den Ausdruck

$$N_{\mathfrak{k}}(\delta_{\mathfrak{k}}(W)) = \pm(W - W^{(1)})^2 \cdot (W - W^{(2)})^2 \cdots (W^{(r-2)} - W^{(r-1)})^2 \tag{23}$$
$$= \pm \begin{vmatrix} 1, & W, & W^2, & \cdots\cdots, & W^{r-1} \\ 1, & W^{(1)}, & W^{2}_{(1)}, & \cdots\cdots, & W^{r-1}_{(1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & W^{(r-1)}, & W^{2}_{(r-1)}, & \cdots, & W^{r-1}_{(r-1)} \end{vmatrix}^2.$$

Das Determinantenquadrat zur Rechten ist, wie die bei (20) angestellte Überlegung zeigt, eine Form mit den Unbestimmten U_i und mit Koeffizienten, welche zu $\mathfrak{k}$ gehören. Setzt man darin aber für die Potenzen der $W, W^{(1)}, \cdots, W^{(r-1)}$, die N-teiligen Ausdrücke (21) und die zu ihnen relativ konjugierten, so bleiben, wenn zur Entwicklung der Determinante ihre Kolonnen in ihre Bestandteile aufgelöst werden, ersichtlich nur

1) S. Hilberts Bericht über die Theorie der algebraischen Zahlkörper, § 15, 16.

solche Teile bestehen, welche eine der Determinanten der Matrix (20) zum Koeffizienten haben, und hieraus leuchtet ein, daß das Determinantenquadrat (23) lauter durch $\mathfrak{D}_{\mathfrak{k}}$ teilbare Koeffizienten besitzt. Der Teiler des Ausdrucks

$$(24)\qquad (W - W^{(1)})^2 \cdot (W - W^{(2)})^2 \cdots (W^{(r-2)} - W^{(r-1)})^2$$

d. h. $N_{\mathfrak{k}}(D_{\mathfrak{k}})$ geht also auch auf durch $\mathfrak{D}_{\mathfrak{k}}$. Bildet man andererseits irgend eine jener Determinanten der Matrix (20), z. B. die Determinante

$$\Omega = \begin{vmatrix} \Omega_1, & \Omega_2, \cdots\cdots, & \Omega_r \\ \Omega_1^{(1)}, & \Omega_2^{(1)}, \;\cdots, & \Omega_r^{(1)} \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, \cdots, & \Omega_r^{(r-1)} \end{vmatrix},$$

und ersetzt darin die Ω_i und ihre relativ Konjugierten durch die Ausdrücke (22) und die ihnen konjugierten, so erkennt man sogleich, daß $\Omega \cdot U^r$ eine Form mit den Unbestimmten U_i ist, welche durch jede der Differenzen $W^{(i)} - W^{(k)}$ und mithin durch das Produkt

$$(W - W^{(1)}) \cdot (W - W^{(2)}) \cdots (W^{(r-2)} - W^{(r-1)})$$

teilbar ist. Daher geht jedes der Produkte $\Omega^2 \cdot U^{2r}$, worin Ω eine der Determinanten der Matrix (20) ist, durch den Ausdruck (24) und, da U^{2r} eine Einheitsform ist, jedes der Quadrate Ω^2 und somit auch ihr größter gemeinsamer Teiler $\mathfrak{D}_{\mathfrak{k}}$ durch den Teiler von (24), d. i. durch $N_{\mathfrak{k}}(D_{\mathfrak{k}})$ auf. — Hieraus erschließt man den ersten Satz:

Zwischen der Relativdifferente und der Relativdiskriminante des Körpers $\mathfrak{K}$ besteht die Beziehung

$$(25)\qquad \mathfrak{D}_{\mathfrak{k}} = N_{\mathfrak{k}}(D_{\mathfrak{k}}).$$

4. Der zweite spricht sich aus in der Formel

$$(26)\qquad \mathrm{D} = d^r \cdot n(\mathfrak{D}_{\mathfrak{k}}),$$

in welcher D, d die Diskriminanten der Körper $\mathfrak{K}$ und $\mathfrak{k}$, und $n(\mathfrak{D}_{\mathfrak{k}})$ die im Körper $\mathfrak{k}$ genommene Norm der Relativdiskriminante $\mathfrak{D}_{\mathfrak{k}}$ bedeuten.

Um ihn zu beweisen, gehen wir auf Kap. 1, Nr. 15 zurück. Ersetzen wir dort α durch die Fundamentalform

$$w = \omega_1 u_1 + \omega_2 u_2 + \cdots + \omega_n u_n$$

des Körpers $\mathfrak{k}$ und A durch diejenige

$$W = \Omega_1 U_1 + \Omega_2 U_2 + \cdots + \Omega_N U_N$$

des Körpers $\mathfrak{K}$, so übersieht man leicht, daß die Diskriminante des letzteren, nämlich der Ausdruck

$$(27)\qquad \begin{vmatrix} 1, & W, & W^2, & \ldots, & W^{N-1} \\ 1, & W^{(1)}, & \overset{2}{W^{(1)}}, & \ldots, & \overset{N-1}{W^{(1)}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & W^{(N-1)}, & \overset{2}{W^{(N-1)}}, & \ldots, & \overset{N-1}{W^{(N-1)}} \end{vmatrix}^2$$

durch das Quadrat des der dortigen Determinante (78) entsprechenden Ausdrucks teilbar wird. In der Tat genügen die zu W relativ konjugierten Formen der Gleichung

$$(28)\qquad (X - W)(X - W^{(1)}) \cdots (X - W^{(r-1)}) = 0,$$

wo die Koeffizienten ganze Funktionen der U_i und symmetrisch in bezug auf die Wurzeln der Gleichung (6) sind, also ihrerseits Koeffizienten haben, welche Zahlen in $\mathfrak{k}$, mithin (vgl. (22)) als Quotienten darstellbar sind mit einer ganzen Funktion von w als Zähler und einer Einheitsform u der Unbestimmten u_i als Nenner; die Gleichung (28) läßt sich daher schreiben wie folgt:

$$(29)\qquad u \cdot X^r + u_1(w) \cdot X^{r-1} + \cdots + u_r(w) = 0,$$

unter $u_i(w)$ ganze, ganzzahlige Funktionen von w und den Unbestimmten u_i, U_i verstanden. Da andererseits die Fundamentalform w selbst einer ganzzahligen Gleichung n^{ten} Grades Genüge leistet, so leuchtet, da W die Gleichung (29) erfüllt, ein, daß jede Potenz von W nach Multiplikation mit einer gewissen Potenz von u sich als lineare Funktion der Größen

$$(30)\qquad \begin{aligned} 1, w, \cdots, w^{n-1}, \quad & W, wW, \cdots, w^{n-1}W, \cdots, \\ & W^{r-1}, wW^{r-1}, \cdots, w^{n-1}W^{r-1} \end{aligned}$$

ausdrücken läßt mit Koeffizienten, welche ganze, ganzzahlige Funktionen der Unbestimmten u_i, U_i sind, und ebenso die Konjugierten dieses Produktes als die konjugierten Ausdrücke des ebengenannten. Die in (27) auftretende Determinante wird

demnach in der Tat dann teilbar durch den Ausdruck, welcher der Determinante (78) des ersten Kapitels analog aus w und W gebildet ist, eine Determinante, die ihrerseits dem Produkte der dortigen Determinanten (81) gleich war. Unter den letzteren verwandelt sich aber für $\alpha = w$ das Quadrat der ersten in die r^{te} Potenz der Diskriminante $\Delta(w)$ der Fundamentalform von $\mathfrak{k}$, während die dann folgende für $A = W$ nach (23) den Ausdruck $N_{\mathfrak{k}}(\partial_{\mathfrak{k}}(W))$ zum Quadrate hat. — Aus alle diesem folgt zunächst, daß die Diskriminante der Fundamentalform von $\mathfrak{K}$ nach Multiplikation mit einer gewissen Potenz der Einheitsform u teilbar wird durch

$$\Delta(w)^r \cdot n N_{\mathfrak{k}}(\partial_{\mathfrak{k}}(W)), \tag{31}$$

daß also der Teiler jenes Produktes, d. i. die Diskriminante D durch denjenigen des letzten Ausdrucks, d. i. durch $d^r \cdot n N_{\mathfrak{k}}(D_{\mathfrak{k}}) = d^r \cdot n(\mathrm{D}_{\mathfrak{k}})$ aufgehen muß.

Umgekehrt sind die Elemente der ersten Reihe in der Determinante (78) des ersten Kapitels für $\alpha = w$, $A = W$, d. h. die Größen (30) lineare Funktionen der Basiszahlen $\Omega_1, \Omega_2, \cdots, \Omega_N$, da auch die Basiszahlen ω_i der Fundamentalform w als in $\mathfrak{k}$ also auch in $\mathfrak{K}$ enthaltene ganze Zahlen in solcher Weise durch die Ω_i ausdrückbar sind; die Elemente der übrigen Reihen jener Determinante sind die gleichen Funktionen der Konjugierten $\Omega_1^{(i)}, \Omega_2^{(i)}, \cdots, \Omega_N^{(i)}$. Daraus folgt, daß jene Determinante eine ganze Funktion der Unbestimmten u_i, U_i ist, welche durch

$$\begin{vmatrix} \Omega_1, & \Omega_2, & \cdots\cdots, & \Omega_N \\ \Omega_1^{(1)}, & \Omega_2^{(1)}, & \cdots\cdots, & \Omega_N^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \Omega_1^{(N-1)}, & \Omega_2^{(N-1)}, & \cdots, & \Omega_N^{(N-1)} \end{vmatrix}$$

teilbar ist, ihr Quadrat also eine solche Funktion, welche durch die Diskriminante D teilbar ist. Da hiernach D ein Teiler des Ausdrucks (31), d. h. von $d^r \cdot n(\mathrm{D}_{\mathfrak{k}})$ sein muß, so folgt in Verbindung mit dem ersterhaltenen Resultate die Gleichheit von D und $d^r \cdot n(\mathrm{D}_{\mathfrak{k}})$, wie sie behauptet worden ist.

Schon Kronecker hat gezeigt (Festschrift § 9), daß die Diskriminante eines Körpers durch diejenige eines jeden seiner

Unterkörper teilbar ist; aber die Formel (26) lehrt genauer, daß sie sogar durch eine gewisse Potenz derselben aufgeht, und läßt zudem erkennen, welche Bedeutung dem Verhältnisse zwischen ihr und dieser Potenz zukommt.

5. Ist

$$\mathrm{F}(X) = X^N + F_1 \cdot X^{N-1} + F_2 \cdot X^{N-2} + \cdots + F_N = 0$$

die Gleichung, welcher die Fundamentalform W des Körpers $\mathfrak{K}$ genügt und deren Koeffizienten ganze und ganzzahlige Funktionen der U_i sind, und bezeichnet man zur Abkürzung die linke Seite der Gleichung (29) mit $f(X, w)$, so ist offenbar

$$(32) \qquad u^n \cdot \mathrm{F}(X) = f(X, w) \cdot f(X, w^{(1)}) \cdots f(X, w^{(n-1)}).$$

Aus dieser Gleichheit folgt durch Differenzierung und mit Rücksicht darauf, daß W eine Wurzel der Gleichung (29) ist,

$$(33) \qquad u^n \cdot \partial(W) = \frac{\partial f(W, w)}{\partial W} \cdot f(W, w^{(1)}) \cdots f(W, w^{(n-1)}).$$

Setzt man nun

$$(34) \qquad f(W, w^{(i)}) = f(W, w^{(i)}) - f(W, w) = (w - w^{(i)}) \cdot Q_i,$$

wo Q_i eine ganze Funktion der Unbestimmten u_i, U_i bedeutet, so nimmt die Gleichung (33) die Gestalt an:

$$u^{n-1} \cdot \partial(W) = \frac{1}{u} \cdot \frac{\partial f(W, w)}{\partial W} \cdot (w - w^{(1)}) \cdots (w - w^{(n-1)}) \cdot Q_1 \cdots Q_{n-1},$$

in welcher nun der erste Faktor

$$\frac{1}{u} \cdot \frac{\partial f(W, w)}{\partial W}$$

die Relativdifferente $\partial_{\mathfrak{k}}(W)$, der zweite Faktor

$$(w - w^{(1)}) \cdots (w - w^{(n-1)})$$

die Differente $\partial(w)$ bedeutet, Formen der Unbestimmten u_i, U_i, welche resp. den Inhalt $D_{\mathfrak{k}}$ und $\mathfrak{d}$ besitzen, wenn $\mathfrak{d}$ die Differente oder das Grundideal des Körpers $\mathfrak{k}$ bezeichnet. Nennt man daher $\mathfrak{q}$ den Inhalt des Produktes $Q_1 Q_2 \cdots Q_{n-1}$, so findet sich aus vorstehender Formel der Inhalt $\mathfrak{D}$ der Differente $\partial(W)$ durch die Gleichung

$$(35) \qquad \mathfrak{D} = D_{\mathfrak{k}} \cdot \mathfrak{d} \cdot \mathfrak{q},$$

aus welcher durch den Übergang zur Norm die andere:

$$N(\mathfrak{D}) N(D_{\mathfrak{k}}) \cdot N(=\mathfrak{d}) \cdot N(\mathfrak{q})$$

hervorgeht. Da aber einerseits die Norm der Differente von $\mathfrak{K}$ gleich der Diskriminante D dieses Körpers, andererseits

$$N(D_{\mathfrak{k}}) = n N_{\mathfrak{k}}(D_{\mathfrak{k}}) = n(\mathrm{D}_{\mathfrak{k}}),$$

endlich

$$N(\mathfrak{d}) = n(\mathfrak{d}^r) = n(\mathfrak{d})^r = d^r$$

ist, muß wegen (26) $N(\mathfrak{q}) = 1$, d. h. $\mathfrak{q}$ dasjenige Ideal des Körpers $\mathfrak{K}$ sein, welches alle ganzen Zahlen desselben enthält, und die Formel (35) nimmt die einfachere Gestalt an:

$$\mathfrak{D} = \mathfrak{d} \cdot D_{\mathfrak{k}} \tag{36}$$

und lehrt den durch seine Einfachheit bemerkenswerten Satz:

Man erhält die Differente des Körpers $\mathfrak{K}$ aus der Differente seines Unterkörpers $\mathfrak{k}$, wenn man diese mit der auf $\mathfrak{k}$ bezüglichen Relativdifferente von $\mathfrak{K}$ multipliziert.

Das vom Ideale $\mathfrak{q}$ Bewiesene besagt endlich, daß jede der Formen $Q_1, Q_2, \cdots, Q_{n-1}$ eine Einheitsform sein muß. Da nun aus (28), (29)

$$f(W, w^{(i)}) = u \cdot (W - W_i)(W - W_i^{(1)}) \cdots (W - W_i^{(r-1)})$$

gefolgert werden kann, wenn $W_i, W_i^{(1)}, \cdots, W_i^{(r-1)}$ die den Wurzeln der Gleichung (7) entsprechenden Werte der Fundamentalform W sind, so gibt die Vergleichung dieses Ausdrucks mit dem Ausdrucke (34) unmittelbar die folgende Äquivalenz

$$w - w^{(i)} \sim (W - W_i)(W - W_i^{(1)}) \cdots (W - W_i^{(r-1)}), \tag{37}$$

welche bei der Vertauschbarkeit der Glieder $w, w^{(i)}$ der Differenz auch durch diese:

$$w - w^{(i)} \sim (W_i - W)(W_i - W^{(1)}) \cdots (W_i - W^{(r-1)}) \tag{37a}$$

ersetzt werden darf. Bedenkt man nun, daß der Inhalt von $w - w^{(i)}$ das „Element" $\mathfrak{e}^{(i)}$ des Körpers $\mathfrak{k}$ ist, während die Faktoren zur Rechten der Formeln gewisse „Elemente" des Körpers $\mathfrak{K}$ zum Inhalte haben, so findet man schließlich den Satz:

Jedes Element $\mathfrak{e}^{(i)}$ des Unterkörpers $\mathfrak{k}$ zerlegt sich

nach den Formeln (37), (37ᵃ) im Oberkörper $\mathfrak{K}$ in ein Produkt von r Idealfaktoren, welche Elemente des letztern sind.

6. Wir wollen nun einen Körper $\mathfrak{K}$ vom N^{ten} Grade betrachten, der aus zwei andern Körpern $\mathfrak{k}$, $\bar{\mathfrak{k}}$ von den Graden n, $\bar{n}$ zusammengesetzt ist, diese mithin als Unterkörper in sich enthält. Dann gilt vor allem der Satz:

Die Diskriminante von $\mathfrak{K}$ besteht aus denselben Primfaktoren, aus welchen insgesamt diejenigen von $\mathfrak{k}$ und $\bar{\mathfrak{k}}$ zusammengesetzt sind. Denn nach (26) bestehen die beiden Gleichungen

$$D = d^r \cdot n(D_{\mathfrak{k}}), \quad D = \bar{d}^{\bar{r}} \cdot \bar{n}(D_{\bar{\mathfrak{k}}}), \tag{38}$$

wenn d, $\bar{d}$ die Diskriminanten von $\mathfrak{k}$, $\bar{\mathfrak{k}}$ und $D_{\mathfrak{k}}$, $D_{\bar{\mathfrak{k}}}$ die Relativdiskriminanten von $\mathfrak{K}$ mit bezug auf diese beiden Unterkörper sind, während

$$N = r \cdot n = \bar{r} \cdot \bar{n} \tag{39}$$

gesetzt ist und $n(D_{\mathfrak{k}})$, $\bar{n}(D_{\bar{\mathfrak{k}}})$ die in $\mathfrak{k}$ und $\bar{\mathfrak{k}}$ genommenen Normen von $D_{\mathfrak{k}}$, $D_{\bar{\mathfrak{k}}}$ resp. bezeichnen. Die Formeln (38) lassen erkennen, daß jedenfalls die genannten Primzahlen in der Diskriminante D aufgehen; es bleibt aber noch zu zeigen, daß D keine anderen Primfaktoren weiter besitzt. Zu diesem Zwecke bezeichne man mit α eine der den Körper $\mathfrak{k}$ erzeugenden ganzen Zahlen und mit $\bar{\omega}_1, \bar{\omega}_2, \cdots, \omega_{\bar{n}}$ eine Basis für die Gesamtheit seiner ganzen Zahlen. Nach Kap. 1, Nr. 10 ist dann α Wurzel einer in $\mathfrak{k}$ irreduktibeln Gleichung r^{ten} Grades (wo $r \gtreqless \bar{n}$)

$$x^r + k_1(\alpha)\, x^{r-1} + \cdots + k_r(\alpha) = 0, \tag{40}$$

deren Koeffizienten Zahlen des durch α erzeugten Körpers $\mathfrak{k}$ sind, und aus deren Wurzeln der Körper $\mathfrak{K}$ und seine relativ zu $\mathfrak{k}$ Konjugierten (vgl. das zur Gleichung (6) Gesagte) entstehen. Geht mithin $\mathfrak{K}$ in einen seiner relativ Konjugierten $\mathfrak{K}^{(i)}$, also $\Omega_1, \Omega_2, \cdots, \Omega_N$ in $\Omega_1^{(i)}, \Omega_2^{(i)}, \cdots, \Omega_N^{(i)}$ über, so verwandeln sich die Basiszahlen $\bar{\omega}_1, \bar{\omega}_2, \cdots, \bar{\omega}_{\bar{n}}$ in diejenigen $\omega_1^{(i)}, \omega_2^{(i)}, \cdots, \omega_{\bar{n}}^{(i)}$ eines der zu $\bar{\mathfrak{k}}$ konjugierten, von ihm verschiedenen Körpers. Da nun die Basiszahlen $\bar{\omega}_i$ ganze Zahlen

in $\mathfrak{K}$ sind, mithin Gleichungen bestehen von der folgenden Gestalt:

$$\omega_h = c_{h1}\Omega_1 + c_{h2}\Omega_2 + \cdots + c_{hN}\Omega_N$$
$$(h = 1, 2, \cdots, \bar{n})$$

und daher auch die folgenden:

$$\bar{\omega}_h^{(i)} = c_{h1}\Omega_1^{(i)} + c_{h2}\Omega_2^{(i)} + \cdots + c_{hN}\Omega_N^{(i)},$$
$$(h = 1, 2, \cdots, \bar{n})$$

so schließt man sogleich, daß die Determinanten der Matrix

$$\begin{Vmatrix} \bar{\omega}_1, & \bar{\omega}_2, & \cdots\cdots, & \omega_{\bar{n}} \\ \omega_1^{(1)}, & \omega_2^{(1)}, & \cdots, & \bar{\omega}_{\bar{n}}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \omega_1^{(r-1)}, & \bar{\omega}_2^{(r-1)}, & \cdots, & \bar{\omega}_{\bar{n}}^{(r-1)} \end{Vmatrix}$$

lineare ganzzahlige Funktionen derjenigen der Matrix (20) sind. Jeder gemeinsame Idealteiler der letzteren geht also auch in jeder von jenen, und da die Determinante

$$\begin{vmatrix} \bar{\omega}_1, & \bar{\omega}_2, & \cdots\cdots, & \bar{\omega}_{\bar{n}} \\ \omega_1^{(1)}, & \bar{\omega}_2^{(1)}, & \cdots\cdots, & \bar{\omega}_{\bar{n}}^{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ \bar{\omega}_1^{(\bar{n}-1)}, & \omega_2^{(\bar{n}-1)}, & \cdots, & \bar{\omega}_{\bar{n}}^{(\bar{n}-1)} \end{vmatrix}$$

als eine lineare Funktion derselben darstellbar ist, auch in dieser Determinante auf. Daher ist deren Quadrat, d. h. die Diskriminante $\bar{d}$ teilbar durch $D_{\mathfrak{k}}$, und somit enthält $D_{\mathfrak{k}}$ keinen Idealteiler und daher $n(D_{\mathfrak{k}})$ keinen rationalen Primfaktor, der nicht auch aufginge in d. Im Hinblick auf (38) ist hiernach die Behauptung des Satzes vollständig erwiesen.

Da dieser Satz ersichtlich auf einen Körper ausgedehnt werden darf, der aus mehr als zwei anderen zusammengesetzt ist, so fließt aus ihm als unmittelbare Folgerung der andere Satz: Die Diskriminante des *Galois*schen Körpers, der aus allen Konjugierten $\mathfrak{k}, \mathfrak{k}^{(1)}, \mathfrak{k}^{(2)}, \cdots, \mathfrak{k}^{(n-1)}$ eines Körpers $\mathfrak{k}$ vom Grade n zusammengesetzt ist, besteht aus denselben Primzahlen, wie diejenige von $\mathfrak{k}$, denn die Diskriminanten der konjugierten Körper sind sämtlich die Diskriminante von $\mathfrak{k}$.

7. Die genauere Art und Weise, wie sich die Diskriminante des zusammengesetzten Körpers aus den Primfaktoren derjenigen der ihn zusammensetzenden Körper bildet, hat Hensel für den ausgezeichneten Fall ermittelt, daß der Grad jenes Körpers gleich dem Produkte aus den Graden der letzteren:

$$N = n \cdot \bar{n} \tag{41}$$

ist.[1])

Dieser Fall tritt z. B. immer ein, wenn die *Grade* n, $\bar{n}$ der zusammensetzenden Körper relativ prim sind. Denn nach (39) muß rn teilbar sein durch $\bar{n}$; mithin ist im gedachten Falle r teilbar durch $\bar{n}$, und da $r \lessgtr \bar{n}$ ist, muß $r = \bar{n}$ also $N = n \cdot \bar{n}$ sein.

Der gleiche Fall tritt ein, wenn die *Diskriminanten* der beiden zusammensetzenden Körper relativ prim sind. Dies beweist sich (nach Hilbert, Bericht § 52) folgendermaßen. Seien $\mathfrak{k}$, $\bar{\mathfrak{k}}$ die beiden, den Körper $\mathfrak{K}$ zusammensetzenden Körper, d, $\bar{d}$ ihre zu einander primen Diskriminanten und $\bar{K}$ der Galoissche Körper, welcher aus den sämtlichen mit $\bar{\mathfrak{k}}$ Konjugierten zusammengesetzt ist, so ist auch dessen Diskriminante $\bar{\mathrm{D}}$ dem letzten Satze der vorigen Nummer zufolge prim gegen d. Bedeutet nun k den Körper, der mit den Koeffizienten der Gleichung (40) rational gebildet ist, so ist derselbe offenbar ein Unterkörper von $\mathfrak{k}$, zugleich aber, da jene Koeffizienten selbst als rational aus $\bar{\alpha}$ und Konjugierten von $\bar{\alpha}$ zusammengesetzte Zahlen dem Körper $\bar{K}$ angehören, auch ein Unterkörper von $\bar{K}$. Die Diskriminante von k wäre daher nach (26) ein gemeinsamer Teiler von d und von der Diskriminante von $\bar{K}$, mithin der Einheit gleich, was dem allgemeinen Satze in Kap. 8, Nr. 7 widerspricht, nach welchem die Diskriminante eines jeden Körpers von 1 verschieden ist, ein Widerspruch, welcher nur fällt, wenn der Grad r der Gleichung (40) gleich $\bar{n}$, diese Gleichung nämlich die irreduktible ganzzahlige Gleichung ist, der der Körper $\bar{\mathfrak{k}}$ entspringt, wo dann k der Körper R der rationalen Zahlen wird.

1) Hensel, über Gattungen, welche durch Komposition aus zwei anderen Gattungen entstehen, Journ. f. Math. 105, p. 329.

Wir setzen nun im folgenden allgemein die Gleichung (41) als erfüllt voraus, beschränken uns aber in der Darstellung der Henselschen Betrachtungen auf den Fall einer Primzahl p, welche weder für den Körper $\mathfrak{k}$, noch für den Körper $\bar{\mathfrak{k}}$ zu den singulären (s. Kap. 7, Nr. 18) gehört.

Vor allem sei dann bemerkt, daß stets n ganze Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ des Körpers $\mathfrak{k}$ so gewählt werden können, daß sie in bezug auf die gegebene Primzahl p unabhängig sind, daß nämlich eine ganzzahlige Kongruenz

$$(42)\qquad u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n \equiv 0 \pmod{p}$$

nur dann stattfinden kann, wenn sämtliche u_i durch p teilbar sind; jede Basis aller ganzen Zahlen in $\mathfrak{k}$ würde ein solches System, doch braucht nicht auch das Umgekehrte der Fall zu sein. Wenn die Zahlen ω_i diese Bedingung erfüllen, so sollen sie ein Fundamentalsystem von $\mathfrak{k}$ (mod. p) genannt werden. Ein besonders geartetes System dieser Art läßt sich unschwer folgendermaßen den Resultaten des 6. Kapitels entnehmen. Sei nämlich

$$(43)\qquad p = \mathfrak{p}_1^{a_1}\cdot\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_m^{a_m}$$

die Zerlegung der Primzahl p in ihre Primfaktoren im Körper $\mathfrak{k}$ und $f_1, f_2, \cdots, f_m$ die Grade von $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_m$, sodaß die Gleichung besteht

$$(44)\qquad a_1f_1 + a_2f_2 + \cdots + a_mf_m = n;$$

wir setzen außerdem noch

$$(45)\qquad f_1 + f_2 + \cdots + f_m = n_1$$

und bezeichnen mit $\mathfrak{p}_{i1}, \mathfrak{p}_{i2}, \cdots, \mathfrak{p}_{in}$ die n mit $\mathfrak{p}_i$ konjugierten Ideale, sodaß $\mathfrak{p}_{i1}$ identisch ist mit $\mathfrak{p}_i$. Dann gibt es im Körper $\mathfrak{k}$ nach Kap. 6, Nr. 18 f_i (mod. $\mathfrak{p}_i$) unabhängige ganze Zahlen

$$(46)\qquad \xi_{i1}, \xi_{i2}, \cdots, \xi_{if_i}.$$

Bildet man daher für jeden Index $i = 1, 2, \cdots, m$ die a_if_i Produkte

$$(47)\qquad \frac{p}{\mathfrak{p}_{i1}^{a_i-h_i}}\cdot\xi_{i1}, \quad \frac{p}{\mathfrak{p}_{i1}^{a_i-h_i}}\cdot\xi_{i2}, \quad\cdots,\quad \frac{p}{\mathfrak{p}_{i1}^{a_i-h_i}}\cdot\xi_{if_i},$$
$$(h_i = 0, 1, 2, \cdots, a_i - 1)$$

so stellt ihre Gesamtheit, deren Anzahl wegen (44) gleich n ist, ein Fundamentalsystem des Körpers $\mathfrak{k}$ (mod. p) dar. Denn, bestände zwischen diesen n Zahlen eine ganzzahlige Kongruenz (mod. p), so bestände sie umsomehr auch (mod. $\mathfrak{p}_i^{a_i}$); dies ergäbe, da die Multiplikatoren der ξ_{hk} für einen von i verschiedenen Wert des Index h durch $\mathfrak{p}_i^{a_i}$ teilbar sind, eine ganzzahlige Kongruenz zwischen den Größen (47) (mod. $\mathfrak{p}_i^{a_i}$) also auch (mod. $\mathfrak{p}_i$), und folglich, da die Glieder, deren Multiplikatoren durch $\mathfrak{p}_i$ aufgehen, weggelassen werden können, eine solche Kongruenz auch zwischen den Zahlen (46), deren ganzzahlige Koeffizienten also durch p teilbar sein müßten. Betrachtet man dann dieselben Kongruenzen (mod. $\mathfrak{p}_i^2$), so stellen sich wieder die Koeffizienten von f_i weiteren Gliedern als teilbar durch p heraus, usw.

Ein Fundamentalsystem des Körpers (mod. p) ist stets auch eine Basis desselben. Denn, bestände für ein solches System $\omega_1, \omega_2, \cdots, \omega_n$ die ganzzahlige Gleichung

$$u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n = 0,$$

so folgte daraus auch die Kongruenz

$$u_1\omega_1 + u_2\omega_2 + \cdots + u_n\omega_n \equiv 0 \pmod{p},$$

mithin allgemein $u_i = p \cdot v_i$ und folglich die Gleichung

$$v_1\omega_1 + v_2\omega_2 + \cdots + v_n\omega_n = 0,$$

aus der nun in gleicher Weise wieder allgemein $v_i = p \cdot w_i$ sich ergäbe, usw. fort, was nur möglich ist, wenn alle Zahlen u_i gleich Null sind.

Indessen brauchen die Zahlen $\omega_1, \omega_2, \cdots, \omega_n$ des Fundamentalsystems (mod. p) nicht zugleich auch Basiszahlen für die Gesamtheit der ganzen Zahlen des Körpers zu sein. Immer aber werden sie, wenn $\gamma_1, \gamma_2, \cdots, \gamma_n$ solche Basiszahlen sind, mit diesen durch n lineare ganzzahlige Gleichungen verbunden sein, deren Determinante durch p nicht aufgehen kann, da sonst nach Kap. 1, Nr. 7 eine ganzzahlige Kongruenz (mod. p) zwischen den ω_i bestände, deren Koeffizienten nicht sämtlich durch p teilbar wären. Hieraus ergibt sich offenbar die Diskriminante der ω_i gleich derjenigen der γ_i (d. i. gleich der Diskriminante d des Körpers $\mathfrak{k}$) mal einer durch p nicht

teilbaren Zahl und demnach enthält die Diskriminante des Fundamentalsystems (mod. p) den Primfaktor p genau so oft, wie diejenige des Körpers, also (für Primzahlen p der vorausgesetzten Art) nach Kap. 7, Nr. 13 genau $n - n_1$ mal.

Insbesondere schließen wir also: das Quadrat der Determinante, welche aus den Größen (47) für $i = 1, 2, \cdots, m$ und aus deren Konjugierten gebildet ist, enthält die Primzahl p genau in der $n - n_1^{\text{ten}}$ Potenz.

8. Nun gilt ein allgemeinerer Satz, der für das Folgende die wesentliche Grundlage abgibt. Sind $\eta_{11}, \eta_{12}, \cdots, \eta_{1n}$ irgend welche n voneinander unabhängige Zahlen des Körpers $\mathfrak{k}$ und bedeuten $\eta_{1k}, \eta_{2k}, \cdots, \eta_{nk}$ die Zahl η_{1k} und ihre Konjugierten, so ist bekanntlich die Determinante $\Delta = | \eta_{ik} |$ von Null verschieden. Die n Elemente jeder Vertikalreihe derselben bilden jedenfalls in dem aus $\mathfrak{k}$ und seinen Konjugierten gebildeten Galoisschen Körper ein Ideal

$$\{\eta_{1k}, \eta_{2k}, \cdots, \eta_{nk}\},$$

welches den größten gemeinsamen Idealteiler der gedachten Elemente darstellt. Dies vorausgeschickt lautet der gemeinte Satz folgendermaßen:

Wenn in der Determinante Δ die Glieder der einzelnen Vertikalreihen durch Potenzen

$$p^{\varrho_1}, p^{\varrho_2}, \cdots, p^{\varrho_n}$$

mit nicht negativen, echt gebrochenen Exponenten teilbar sind und die Summe

$$\varrho = \sum_{i=1}^{n} \varrho_i \tag{48}$$

der letzteren ist zugleich der Exponent der höchsten Potenz von p, durch welche die Determinante Δ selbst aufgeht, so bilden die Zahlen $\eta_{11}, \eta_{12}, \cdots, \eta_{1n}$ ein fundamentales System des Körpers $\mathfrak{k}$ (mod. p). Bestünde nämlich eine ganzzahlige Kongruenz

$$u_1\eta_{11} + u_2\eta_{12} + \cdots + u_n\eta_{1n} \equiv 0 \pmod{p}$$

d. h. eine Gleichung von der Form

$$u_1 \eta_{11} + u_2 \eta_{12} + \cdots + u_n \eta_{1n} = p \cdot \eta_1,$$

worin η_1 eine ganze Zahl des Körpers $\mathfrak{k}$, so folgten daraus auch die konjugierten Gleichungen

$$u_1 \eta_{i1} + u_2 \eta_{i2} + \cdots + u_n \eta_{in} = p \cdot \eta_i, \quad (i = 1, 2, \cdots, n)$$

durch deren Auflösung sich ergäbe

$$\Delta \cdot u_i = \Delta^{(i)}, \quad (i = 1, 2, \cdots, n) \tag{49}$$

wenn unter $\Delta^{(i)}$ die Determinante verstanden wird, welche aus Δ entsteht, wenn ihre i^{te} Vertikalreihe durch die Zahlen $p\eta_1$, $p\eta_2, \cdots, p\eta_n$ ersetzt wird. Da nun die Elemente der i^{ten} Vertikalreihe in Δ wegen der Bedingung (48) gleichzeitig nur durch $p^{\varrho_i} < p$, diejenigen in $\Delta^{(i)}$ aber durch p teilbar sind, so leuchtet ein, daß $\Delta^{(i)}$ durch eine höhere Potenz von p teilbar sein muß als Δ, daß also wegen (49) jede der Größen u_i einen Teiler mit p gemeinsam haben d. h., da sie rationale ganze Zahlen sind, durch p teilbar sein müssen. Das System der Zahlen $\eta_{11}, \eta_{12}, \cdots, \eta_{1n}$ ist daher in der Tat ein Fundamentalsystem (mod. p).

Ein Fundamentalsystem von dieser Beschaffenheit soll ein *normales* Fundamentalsystem (mod. p) heißen.

Hiernach erkennt man zunächst leicht, daß das in voriger Nummer nachgewiesene Fundamentalsystem (mod. p) solch' ein normales Fundamentalsystem ist. Betrachtet man nämlich in seiner Determinante irgend eine der Vertikalreihen, etwa die Reihe der Glieder

$$\frac{p}{\mathfrak{p}_{i1}^{a_i - h_i}} \cdot \xi_{ik}, \quad \frac{p}{\mathfrak{p}_{i2}^{a_i - h_i}} \cdot \xi_{ik}^{(1)}, \quad \cdots, \quad \frac{p}{\mathfrak{p}_{in}^{a_i - h_i}} \cdot \xi_{ik}^{(n-1)},$$

in denen durch die oberen Indizes (1), (2), $\cdots$, $(n-1)$ die Konjugierten von ξ_{ik} angedeutet sind, so bilden die Multiplikatoren dieser Konjugierten in dem aus $\mathfrak{k}$ und seinen Konjugierten zusammengesetzten Galoisschen Körper ein Ideal

$$\left\{ \frac{p}{\mathfrak{p}_{i1}^{a_i - h_i}}, \frac{p}{\mathfrak{p}_{i2}^{a_i - h_i}}, \cdots, \frac{p}{\mathfrak{p}_{in}^{a_i - h_i}} \right\}, \tag{50}$$

welches den größten gemeinsamen Idealteiler der Multiplikatoren vorstellt und daher jedenfalls ein gemeinsamer Idealteiler aller Elemente jener Vertikalreihe ist. Dies Ideal ist aber äquivalent mit einer gewissen nicht negativen, echt gebrochenen Potenz von p. Denn, ist $\mathfrak{P}_{h_i}$ der größte gemeinsame Teiler der Multiplikatoren, so ist $\mathfrak{P}_{h_i}^{a_i}$ derjenige ihrer a_i^{ten} Potenzen:

$$\mathfrak{P}_{h_i}^{a_i} = \left\{ \frac{p^{a_i}}{\mathfrak{p}_{i1}^{a_i(a_i-h_i)}}, \cdots, \frac{p^{a_i}}{\mathfrak{p}_{in}^{a_i(a_i-h_i)}} \right\}$$
$$= p^{h_i} \cdot \left\{ \left(\frac{p}{\mathfrak{p}_{i1}^{a_i}}\right)^{a_i-h_i}, \cdots, \left(\frac{p}{\mathfrak{p}_{in}^{a_i}}\right)^{a_i-h_i} \right\}.$$

Da nun immer je eins von den Elementen dieses letzten Ideals einen der konjugierten Faktoren $\mathfrak{p}_{i1}, \mathfrak{p}_{i2}, \cdots, \mathfrak{p}_{in}$ von p, deren Produkt gleich p^{f_i} ist, nicht enthält, so ist das Ideal zu jedem dieser Faktoren also auch zu ihrem Produkte, d. h. auch zu p_{h_i} relativ prim, und deshalb $\mathfrak{P}_{h_i}^{a_i}$ mit p^{h_i} und $\mathfrak{P}_{h_i}$ selbst mit $p^{\frac{h_i}{a_i}}$ in bezug auf die Teilbarkeit durch Idealfaktoren von p äquivalent. Die betrachtete Vertikalreihe der Determinante hat demnach den Teiler $p^{\frac{h_i}{a_i}}$, und der gleiche Teiler kommt jeder der f_i Vertikalreihen zu, welche den Gliedern (47) entsprechen. Daher hat die Determinante die erste Eigenschaft der Determinante Δ des Hilfssatzes, und zwar sind die Werte der ϱ_i die folgenden:

$$f_i \text{ mal die Werte } 0,\ \frac{1}{a_i},\ \frac{2}{a_i},\ \cdots,\ \frac{a_i-1}{a_i}$$
$$(\text{für } i = 1, 2, \cdots, m)$$

deren Summe

$$\sum_{i=1}^{m} f_i \cdot \frac{a_i(a_i-1)}{2a_i} = \frac{1}{2}(n - n_1)$$

ist; ebenso groß ist aber (s. vorige Nummer) auch der Exponent der höchsten Potenz von p, welche in der Determinante des nachgewiesenen Fundamentalsystems (mod. p) aufgeht, also ist auch die Bedingung (48) des Hilfssatzes erfüllt, und jenes Fundamentalsystem in der Tat ein normales.

Da $\mathfrak{P}_{h_i}$ für $h_i = 0$ relativ prim gegen p ist, so haben (mit

Rücksicht auf die stattfindende Gleichung (48)) diejenigen Vertikalreihen, welche den Gliedern (47) für $h_i = 0$ entsprechen, keine gemeinsamen Teiler mit p und tragen daher zu der Potenz von p, welche in der Determinante des ganzen Fundamentalsystems aufgeht, nichts bei. Da dies für jeden der Indizes $i = 1, 2, \cdots, m$ gilt, so gibt es

$$f_1 + f_2 + \cdots + f_m = n_1$$

Vertikalreihen, welche prim zu p sind. Denkt man sich die aus diesen Vertikalreihen oder auch nur einem Teile derselben gebildete Matrix, so müssen auch deren Determinanten, von welchen diejenige des gesamten Fundamentalsystems eine lineare Funktion ist, ein zu p relativ primes System bilden, wohingegen die Determinanten jeder Matrix von mehr als n_1 Reihen, weil wenigstens eine der letzteren mit p einen gemeinsamen Teiler haben würde, kein zu p relativ primes System mehr bilden können. Nennt man daher eine Determinante vom Range r, wenn alle Unterdeterminanten, deren Grad eine bestimmte Zahl $\overline{\gtrless} r$ ist, aber nicht mehr diejenigen, deren Grad eine solche Zahl $> r$ ist, ein gegen p primes System bilden, so ist der Rang des gedachten Fundamentalsystems gleich n_1.

Da nun die Elemente eines jeden Fundamentalsystems (mod. p) mit den Basiszahlen γ_i der ganzen Zahlen des Körpers $\mathfrak{k}$, wie schon bemerkt, durch ganzzahlige lineare Gleichungen verbunden sind, deren Determinante durch p nicht teilbar ist, so werden auch (mod. p) umgekehrt die γ_i als ganzzahlige lineare Funktionen jener Elemente darstellbar sein; und, weil dann die s-reihigen Determinanten der aus jenem Fundamentalsystem und seinen Konjugierten gebildeten Determinante lineare Funktionen der aus den γ_i und ihren Konjugierten gebildeten s-reihigen Determinanten sein werden, wie (mod. p) auch umgekehrt, so erkennt man sofort, daß der Rang (mod. p) der aus den γ_i und ihren Konjugierten gebildeten Determinante dem Range jener Determinante gleich sein muß. Man darf hiernach den folgenden Satz aussprechen:

Die Diskriminante des Körpers $\mathfrak{k}$ vom n^{ten} Grade ist genau teilbar durch p^{n-n_1}, wenn die Determinante, deren Quadrat sie ist, (mod. p) vom Range n_1 ist.

9. Wir kehren jetzt zu unserm Vorhaben zurück, die Diskriminante des Körpers $\mathfrak{K}$ vom N^{ten} Grade zu untersuchen, der aus den Körpern $\mathfrak{k}$, $\bar{\mathfrak{k}}$ von den Graden n, $\bar{n}$ zusammengesetzt ist, unter der Voraussetzung, daß die Beziehung

$$N = n \cdot \bar{n}$$

stattfinde. Bei dieser Voraussetzung bleibt (s. Kap. 1, Nr. 10) die ganzzahlige Gleichung $\bar{n}^{\text{ten}}$ Grades, der die den Körper $\bar{\mathfrak{k}}$ erzeugende Zahl $\bar{\alpha}$ genügt, auch nach Adjunktion der den Körper $\mathfrak{k}$ erzeugenden Zahl α irreduktibel. Bezeichnet daher

$$\xi_{11}, \xi_{21}, \cdots, \xi_{n1}$$

ein normales Fundamentalsystem (mod. p) von der in Nr. 7 nachgewiesenen Art für die ganzen Zahlen des Körpers $\mathfrak{k}$,

$$\eta_{11}, \eta_{21}, \cdots, \eta_{\bar{n}1}$$

ein solches für die ganzen Zahlen des Körpers $\bar{\mathfrak{k}}$, ferner wieder $\xi_{i1}, \xi_{i2}, \cdots, \xi_{in}$ bezw. $\eta_{i1}, \eta_{i2}, \cdots, \eta_{i\bar{n}}$ die zu ξ_{i1}, η_{i1} mit bezug auf $\mathfrak{k}$ resp. $\bar{\mathfrak{k}}$ konjugierten Zahlen, und bildet man die $N = n \cdot \bar{n}$ Produkte

$$\xi_{11}\eta_{11}, \xi_{11}\eta_{21}, \cdots, \xi_{11}\eta_{\bar{n}1}, \xi_{21}\eta_{11}, \cdots, \xi_{n1}\eta_{\bar{n}1}, \tag{51}$$

so werden die mit bezug auf den Körper $\mathfrak{K}$ zu ihnen konjugierten Zahlen die folgenden sein:

$$\xi_{1h}\eta_{1l}, \xi_{1h}\eta_{2l}, \cdots, \xi_{1h}\eta_{\bar{n}l}, \xi_{2h}\eta_{1l}, \cdots, \xi_{nh}\eta_{\bar{n}l},$$
$$(\text{für } h = 1, 2, \cdots, n;\ l = 1, 2, \cdots, \bar{n})$$

und, wie man sich unschwer überzeugt, sind die N Zahlen (51) unabhängige Zahlen des Körpers $\mathfrak{K}$. Für die aus ihnen und ihren Konjugierten zusammengesetzte Determinante N^{ten} Grades

$$|\xi_{ih} \cdot \eta_{kl}| \qquad \begin{pmatrix} i, h = 1, 2, \cdots, n \\ k, l = 1, 2, \cdots, \bar{n} \end{pmatrix}$$

gilt analog mit dem von der Determinante (78) des ersten Kapitels Bemerkten, wie zuerst Kronecker in seinen Vorlesungen ausgeführt hat[1]), die Beziehung:

1) Vgl. Hensel, über Gattungen, welche durch Komposition etc., Journ. f. Math. 105, p. 337; ferner Acta Math. 14, p. 317.

$$(52)\qquad |\xi_{ik}\cdot\eta_{kl}| = |\xi_{ik}|^{\bar{n}}\cdot|\eta_{kl}|^{n}.$$

Mit p^{ϱ_i} werde nun wieder die höchste Potenz von p bezeichnet, durch welche alle Glieder in der i^{ten} Vertikalreihe der Determinante $|\xi_{ik}|$, und ebenso mit p^{σ_i} diejenige, durch welche alle Glieder in der i^{ten} Vertikalreihe der Determinante $|\eta_{kl}|$ teilbar sind. Dann bestehen die Gleichungen

$$(53)\qquad 2\cdot\sum_{i=1}^{n}\varrho_i = n - n_1,\quad 2\cdot\sum_{i=1}^{\bar{n}}\sigma_i = \bar{n} - \bar{n}_1,$$

wenn $\bar{n}_1$ die analoge Bedeutung für den Körper $\bar{\mathfrak{k}}$ hat, wie n_1 für den Körper $\mathfrak{k}$, mithin den Rang (mod. p) der Determinante $|\eta_{kl}|$ bestimmt; die Differenzen $n - n_1$, $\bar{n} - \bar{n}_1$ bezeichnen zugleich die Exponenten der höchsten Potenzen von p, welche in den Quadraten der Determinanten $|\xi_{ik}|$, $|\eta_{kl}|$ resp. aufgehen. Nun enthalten die Glieder derjenigen Vertikalreihe der Determinante (52), welche durch die Indizes i, k bezeichnet wird, offenbar die Potenz $p^{\varrho_i+\sigma_k}$ zu gemeinsamem Teiler, und da die auf alle Kombinationen i, k ausgedehnte Summe

$$\sum(\varrho_i+\sigma_k) = \bar{n}\cdot\sum_{i=1}^{n}\varrho_i + n\cdot\sum_{k=1}^{\bar{n}}\sigma_k$$
$$= \bar{n}\cdot\frac{n-n_1}{2} + n\cdot\frac{\bar{n}-\bar{n}_1}{2}$$

d. h. nach (52) gleich dem Exponenten der höchsten Potenz von p ist, welche in der Determinante $|\xi_{ik}\cdot\eta_{kl}|$ selbst aufgeht, so würden die Zahlen (51) ein normales Fundamentalsystem (mod. p) für den Körper $\mathfrak{K}$ bilden, falls die Exponenten $\varrho_i + \sigma_k$ kleiner als 1 wären. Bedeutet aber in üblicher Weise $[\varrho_i + \sigma_k]$ die größte ganze Zahl, welche in $\varrho_i + \sigma_k$ enthalten ist, eine Zahl, welche nur Null oder Eins sein kann, da ϱ_i, σ_k echte Brüche bezeichnen, so wird die Differenz

$$\varrho_i + \sigma_k - [\varrho_i + \sigma_k]$$

gewiß ein nicht negativer echter Bruch sein, und man erkennt daher, daß das aus den Zahlen

$$(54)\qquad \frac{\xi_{i1}\cdot\eta_{k1}}{p^{[\varrho_i+\sigma_k]}}\quad\begin{pmatrix} i = 1, 2, \cdots, n \\ k = 1, 2, \cdots, \bar{n}\end{pmatrix}$$

gebildete System ein normales Fundamentalsystem (mod. p) für den Körper $\mathfrak{K}$ darstellt.

Nennt man nun N_1 den Rang der aus diesem Fundamentalsysteme und seinen Konjugierten gebildeten Determinante, so ist dem Satze am Schlusse voriger Nummer zufolge

$$p^{N-N_1}$$

die höchste Potenz von p, welche in der Diskriminante des Körpers $\mathfrak{K}$ aufgeht. Weil es sich aber um ein normales Fundamentalsystem (mod. p) handelt, so bezeichnet N_1 die Anzahl der Vertikalreihen jener Determinante, welche ohne gemeinsamen Teiler mit p sind, und offenbar entsprechen diese Vertikalreihen denjenigen Gliedern (54) des Fundamentalsystems, bei denen

$$\varrho_i + \sigma_k = [\varrho_i + \sigma_k] \tag{55}$$

ist. Es bleibt also die Anzahl solcher Glieder zu bestimmen. Nun seien

$$p = \mathfrak{p}_1^{a_1} \cdot \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_m^{a_m}, \quad p = \pi_1^{b_1} \cdot \pi_2^{b_2} \cdots \pi_\mu^{b_\mu}$$

die Zerlegungen der Primzahl p in ihre Primidealfaktoren im Körper $\mathfrak{k}$ resp. $\bar{\mathfrak{k}}$, und

$$f_1, f_2, \cdots, f_m;\ \varphi_1, \varphi_2, \cdots, \varphi_\mu$$

die Grade der einzelnen Primideale in diesen Zerlegungen. Wir betrachten zunächst nur diejenigen Vertikalreihen, welche (vgl. die vorausgesetzte Gestalt (47) der Fundamentalsysteme ξ_{i1}, η_{k1} der Körper $\mathfrak{k}$ und $\bar{\mathfrak{k}}$) einer bestimmten Kombination $\mathfrak{p}_i, \pi_k$ jener Primideale entsprechen. In ihnen sind

$$\frac{h_i}{a_i}, \quad \frac{g_k}{b_k} \quad \begin{pmatrix} h_i = 0, 1, 2, \cdots, a_i - 1 \\ g_k = 0, 1, 2, \cdots, b_k - 1 \end{pmatrix} \tag{56}$$

die Werte der Brüche ϱ_i, σ_k, und da jede der Zahlen h_i genau f_i mal, jede der Zahlen g_k genau φ_k mal vorkommt, so tritt jede Kombination h_i, g_k genau $f_i\varphi_k$ mal auf. Soll aber für die Brüche (56) die Bedingung (55) d. i. die Gleichung

$$\frac{h_i}{a_i} + \frac{g_k}{b_k} = \left[\frac{h_i}{a_i} + \frac{g_k}{b_k}\right] \tag{57}$$

erfüllt sein, so ist notwendig und hinreichend, daß

$$h_i b_k + g_k a_i \equiv 0 \pmod{a_i b_k}$$

sei. Diese Kongruenz erfordert, wenn

$$a_i = a_i' \cdot d_{ik}, \quad b_k = b_k' \cdot d_{ik}$$

gesetzt, nämlich der größte gemeinsame Teiler von a_i, b_k mit d_{ik} bezeichnet wird, daß

$$h_i = a_i' \cdot h_i', \quad g_k = b_k' \cdot g_k'$$

sei, und kommt dann auf die folgende zurück:

$$h_i' + g_k' \equiv 0 \pmod{d_{ik}},$$

welche d_{ik} Lösungen hat. Somit erfüllen d_{ik} Kombinationen h_i, g_k die Bedingung (57), und die Anzahl der, der Kombination $\mathfrak{p}_i$, π_k entsprechenden Vertikalreihen, für welche (55) erfüllt ist, beträgt also $f_i \varphi_k \cdot d_{ik}$. Insgesamt ergibt sich also die Anzahl aller Vertikalreihen, für welche (55) stattfindet, indem man diese Anzahlen für alle Kombinationen $\mathfrak{p}_i$, π_k summiert, und so findet sich

$$N_1 = \sum_{i,k} f_i \varphi_k \cdot d_{ik}.$$

Beachtet man nun die Beziehungen

$$n = a_1 f_1 + a_2 f_2 + \cdots + a_m f_m, \quad \bar{n} = b_1 \varphi_1 + b_2 \varphi_2 + \cdots + b_\mu \varphi_\mu$$
$$n_1 = f_1 + f_2 + \cdots + f_m, \quad \bar{n}_1 = \varphi_1 + \varphi_2 + \cdots + \varphi_\mu,$$

so gehen die nachstehenden Gleichungen hervor:

$$(58) \quad \begin{cases} n - n_1 = \sum_{i=1}^{m} f_i (a_i - 1) \\ \bar{n} - \bar{n}_1 = \sum_{k=1}^{\mu} \varphi_k (b_k - 1) \\ N - N_1 = \sum_{i=1}^{m} \sum_{k=1}^{\mu} f_i \varphi_k (a_i b_k - d_{ik}), \end{cases}$$

welche die höchsten, in den Diskriminanten d, $\bar{d}$, D der drei Körper $\mathfrak{k}$, $\bar{\mathfrak{k}}$, $\mathfrak{K}$ aufgehenden Potenzen der (nicht singulären) Primzahl p bestimmen, wenn in

der letzten von ihnen d_{ik} den größten gemeinsamen Teiler von a_i, b_k bedeutet.

Die dritte dieser Formeln gibt das gesuchte Gesetz, nach welchem die Diskriminante des zusammengesetzten Körpers aus den Primfaktoren derjenigen der ihn zusammensetzenden beiden Körper, soweit sie nicht singulär sind, gebildet wird.

Sind insbesondere die Diskriminanten von $\mathfrak{k}$, $\bar{\mathfrak{k}}$ relativ prim, sodaß eine gegebene Primzahl p, welche in D also in einer der Diskriminanten d, $\bar{d}$, etwa in der ersten von beiden aufgeht, die andere derselben nicht teilt, so müssen die sämtlichen Exponenten b_k gleich 1 und somit auch $d_{ik} = 1$ sein; dadurch geht die dritte der Formeln (58) über in diese:

$$N - N_1 = \sum_{i=1}^{m} \sum_{k=1}^{\mu} f_i(a_i - 1)\,\varphi_k = \bar{n}_1 \cdot (n - n_1)$$

und die Diskriminante D enthält den (nicht singulären) Primfaktor p genau so oft, wie die $\bar{n}^{\text{te}}$ Potenz von d. Ginge die Primzahl p umgekehrt in $\bar{d}$ auf, so wäre sie ebenso oft Faktor von D, wie von der n^{ten} Potenz von $\bar{d}$. Hieraus geht offenbar, wenn für die Körper $\mathfrak{k}$, $\bar{\mathfrak{k}}$ keine singulären Primzahlen vorhanden sind, unter der gemachten Voraussetzung die Gleichung

$$\mathrm{D} = d^{\bar{n}} \cdot \bar{d}^{\,n}$$

hervor.

Diese Gleichung besteht aber unter der gleichen Voraussetzung über die Diskriminanten auch ohne die gemachte, die singulären Primzahlen betreffende Einschränkung. Denn für den nach der Annahme vorliegenden Fall ist $r = \bar{n}$, die Formel (26) also gibt

$$\mathrm{D} = d^{\bar{n}} \cdot n(\mathrm{D}_{\mathfrak{k}}),$$

wo der zweite Faktor nach Nr. 6 nur aus Primfaktoren von $\bar{d}$ zusammengesetzt ist. Da nun aus gleichem Grunde

$$\mathrm{D} = \bar{d}^{\,n} \cdot \bar{n}(\mathrm{D}_{\bar{\mathfrak{k}}})$$

und der zweite Faktor hier nur aus Primfaktoren von d zusammengesetzt ist, so muß, da d und $\bar{d}$ teilerfremd vorausgesetzt sind, notwendig

$$\mathrm{D} = d^{\bar{n}} \cdot \bar{d}^{\,n}$$

sein.

Zwölftes Kapitel.

Der Galoissche Körper.

1. Bis hierher gilt die Arithmetik der Zahlenkörper, die wir entwickelt haben, ganz allgemein, da wir über die besondere Natur des betrachteten Zahlenkörpers keinerlei beschränkende Voraussetzungen gemacht haben, und die uns gestellte Aufgabe könnte mit dem Voraufgehenden als abgeschlossen gelten, indem die Arithmetik spezieller Zahlenkörper einem ferneren Werke vorbehalten bleiben soll. Wenn wir gleichwohl dem jetzigen noch einen Abschnitt über diejenigen besonderen Körper, welche man Galoissche Körper nennt, anschließen, so weichen wir damit nur scheinbar von diesem unserm Vorhaben ab. Dem Galoisschen Körper kommt nämlich die ausgezeichnete Eigenschaft zu, daß zwar einerseits die für ihn giltige Theorie der Ideale mit ihren Folgerungen in der allgemeinen, im vorigen dargestellten Idealtheorie als besonderer Fall mit einbegriffen sein muß, daß aber auch andererseits diese sich wieder aus der Arithmetik des Galoisschen Körpers entwickeln läßt. In der Tat, ist $\mathfrak{k}$ ein ganz beliebiger Zahlenkörper, so ist er als ein Unterkörper in demjenigen Galoisschen Körper enthalten, welcher aus ihm und allen seinen Konjugierten zusammengesetzt ist, und daher entspringen notwendig seine Eigenschaften aus denjenigen dieses Galoisschen Körpers. Die besondere Eigenschaft des letzteren aber, nach der er mit seinen Konjugierten identisch ist, hat zur Folge, daß die fundamentalen Sätze der Idealtheorie für ihn sich sehr viel einfacher nachweisen und so seine Arithmetik sich ungleich leichter entwickeln läßt, wie für den allgemein gedachten Zahlenkörper. Somit könnte sie, wie teilweise schon von Kronecker in seiner Gestaltung der Theorie getan worden ist, zur Grundlage der allgemeinen Arithmetik der Zahlenkörper genommen werden. Zugleich aber ist die Kenntnis der arithmetischen Gesetze des Galoisschen Körpers, wo nicht durchaus erforderlich, doch nützlich, um diejenigen anderer besonderer Körper frei und voll zu beherrschen. Wenn

demnach die hauptsächlichsten dieser Eigenschaften hier noch angefügt werden, so erfährt dadurch nicht nur die Begründung der von uns dargestellten allgemeinen Körpertheorie eine wesentliche Ergänzung, sondern es wird auch eine natürliche Brücke geschlagen zu dem Werke, das als Fortsetzung des vorliegenden geplant ist.

Wir beginnen damit, die algebraische Grundeigenschaft des Galoisschen Körpers $\mathfrak{K}$ festzustellen. Ist A die ihn erzeugende ganze Zahl und

$$F(x) = 0 \tag{1}$$

die irreduktible ganzzahlige Gleichung N^{ten} Grades, deren Wurzel sie ist, N also der Grad des Körpers, so ist bekanntlich jede Zahl des Körpers eine ganze Funktion von A vom $N-1^{\text{ten}}$ Grade mit rationalen Koeffizienten, und man erhält die zu $\mathfrak{K}$ konjugierten Körper, indem man in allen diesen Funktionen A durch jede der übrigen Wurzeln der Gleichung (1) ersetzt. Da aber die Konjugierten eines Galoisschen Körpers mit ihm selbst in der Gesamtheit ihrer Zahlen identisch sind, so ist jede der gedachten Wurzeln selbst eine Zahl desselben und folglich eine rationale Funktion von der einen, beliebig gewählten Wurzel A der Gleichung. Jede Gleichung (1), deren sämtliche Wurzeln durch jede beliebige von ihnen rational ausdrückbar sind, heißt aber eine Galoissche Gleichung, und aus diesem Grunde wird der ihr entsprechende Körper $\mathfrak{K}$, zu dessen Bezeichnung Dedekind den Ausdruck „Normalkörper" eingeführt hat, neuerdings lieber „ein Galoisscher Körper" genannt.

Die N Wurzeln der Gleichung (1) mögen durch

$$\mathrm{A},\ \mathrm{A}^{(1)},\ \mathrm{A}^{(2)},\ \cdots,\ \mathrm{A}^{(N-1)} \tag{2}$$

bezeichnet werden. Dann ist also für $i = 0, 1, 2, \cdots, N-1$

$$\mathrm{A}^{(i)} = f_i(\mathrm{A}), \tag{3}$$

wo $f_i(\mathrm{A})$ eine ganze Funktion von A mit rationalen Koeffizienten bedeutet. Die Substitutionen, durch welche der Körper $\mathfrak{K}$ in seine konjugierten, also in der Gesamtheit ihrer Zahlen mit ihm übereinstimmende Körper übergeht, seien

$$s_0,\ s_1,\ s_2,\ \cdots,\ s_{N-1} \tag{4}$$

und s_0 unter ihnen die identische Substitution, welche die einzelnen Zahlen in $\mathfrak{K}$ nicht ändert. Heißt dann $s_i\gamma$ die Zahl, in welche die Zahl γ des Körpers durch eine solche Substitution s_i übergeht, so wird $s_i \mathrm{A} = \mathrm{A}^{(i)}$ gesetzt werden können und somit die Beziehung bestehen:

$$(5) \qquad s_i \mathrm{A} = f_i(\mathrm{A}).$$

Führt man nun einen Körper $\mathfrak{K}$ durch eine Substitution s in einen andern Körper und diesen wieder durch eine Substitution s' in einen dritten Körper über, so bestimmt der letztere, wie leicht zu erkennen, in dem in Kap. 1, Nr. 9 bezeichneten Sinne wieder eine Substitution des ersten Körpers, welche die aus s und s' zusammengesetzte Substitution oder ihr Produkt $s's$ heißt, wobei im allgemeinen die Ordnung der Faktoren wohl zu beachten ist. Die N Substitutionen (4), welche einem *Galois*schen Körper entsprechen, genießen aber der ausgezeichneten Eigenschaft, daß sie eine Gruppe bilden, das heißt bekanntlich, daß das Produkt je zweier Substitutionen s_i, s_k der Reihe (4), gleichviel ob diese Zeichen zwei verschiedene oder ein- und dieselbe Substitution vorstellen, wieder eine Substitution derselben Reihe ist. Denn die Substitution s_i führt den Körper $\mathfrak{K}$ in einen anderen über, der aus den gleichen Zahlen besteht, dessen Zahlen also rationale Funktionen von A sind; die Substitution s_k des Körpers $\mathfrak{K}$ bedeutet mithin auch eine Substitution des transformierten Körpers, und somit bildet das Produkt $s_k s_i$ beider Substitutionen von $\mathfrak{K}$ wieder eine Substitution von $\mathfrak{K}$. Wird also etwa

$$(6) \qquad s_k s_i = s_h$$

gesetzt, so gilt, da nach (5) die Gleichung

$$s_k s_i \mathrm{A} = f_i(s_k \mathrm{A}) = f_i(f_k(\mathrm{A}))$$

stattfindet, zwischen den rationalen Funktionen f_i, f_k, f_h die Beziehung

$$(7) \qquad f_i(f_k(\mathrm{A})) = f_h(\mathrm{A}).$$

Aus der Zusammensetzung irgend zweier der Substitutionen (4) ergibt sich sogleich auch der Begriff der Potenz s_i^m irgend einer von ihnen als die m-fach wiederholte Substitution s_i.

Die Galoissche Gleichung (1) heißt insonderheit eine Abelsche Gleichung, wenn die Beziehung (7) von der Reihenfolge der Operationen f_i, f_k unabhängig, nämlich

(8) $$f_i(f_k(\mathrm{A})) = f_k(f_i(\mathrm{A}))$$

ist, eine Gleichung, welcher die andere:

(9) $$s_k s_i = s_i s_k,$$

d. i. die Kommutativität der Substitutionen der Gruppe (4) entspricht. Demgemäß heißt der *Galois*sche *Körper* insbesondere ein *Abel*scher *Körper*, wenn die Substitutionen seiner Gruppe vertauschbar sind. Für derartige Gruppen gilt aber der schon bei Gelegenheit der Idealklassen benutzte Kroneckersche Fundamentalsatz (s. Kap. 9, Nr. 5), nach welchem alle Substitutionen der Gruppe als Potenzen und Produkte gewisser fundamentaler Substitutionen $s_1, s_2, \cdots, s_\sigma$, also in der Form

(10) $$s_1^{x_1} s_2^{x_2} \cdots s_\sigma^{x_\sigma}$$

dargestellt werden, wenn darin allgemein x_i alle Zahlen 0, 1, 2, $\cdots$ bis zu einer endlichen Zahl h_i hin durchläuft, derart, daß die Anzahl der Substitutionen der Gruppe

$$N = h_1 h_2 \cdots h_\sigma$$

ist. Die Substitutionen

$$s_i^0 = s_0,\ s_i^1,\ s_i^2,\ \cdots,\ s_i^{h_i - 1}$$

bilden offenbar für sich eine Teil- oder Untergruppe der Gesamtgruppe, die ihres besonderen Charakters wegen, indem $s_i^{h_i}$ wieder gleich s_i^0 usw. sein wird, eine zyklische Gruppe genannt wird; daher ist die gesamte Gruppe eines Abelschen Körpers aus einer Anzahl zyklischer Gruppen zusammengesetzt, deren Grad, d. h. die Anzahl der in ihnen enthaltenen Substitutionen wieder noch als eine Primzahlpotenz vorausgesetzt werden darf (s. die angezogene Stelle). Ist die Gruppe des Abelschen Körpers selbst eine zyklische, so wird auch der Abelsche Körper speziell ein zyklischer Körper genannt.

Alle diese Begriffsbestimmungen, die bisher in absolutem Sinne, d. i. für Körper $\mathfrak{K}$ aufgestellt worden sind, deren Ra-

tionalitätsbereich der Körper R der rationalen Zahlen ist, lassen sich nun auch auf den allgemeineren Fall übertragen, wo dieser Rationalitätsbereich ein beliebiger Unterkörper $\mathfrak{k}$ des Körpers $\mathfrak{K}$, der letztere also ein Relativkörper mit Bezug auf $\mathfrak{k}$ ist. Demnach heißt ein Körper $\mathfrak{K}$ ein relativ Galoisscher Körper mit Bezug auf einen seiner Unterkörper $\mathfrak{k}$, wenn die irreduktible Gleichung

$$(11) \qquad x^r + k_1(\alpha)\cdot x^{r-1} + k_2(\alpha)\cdot x^{r-2} + \cdots + k_r(\alpha) = 0$$

mit in $\mathfrak{k}$ enthaltenen Koeffizienten, der die ihn erzeugende Zahl A genügt, eine Galoissche Gleichung ist, nämlich ihre sämtlichen Wurzeln durch eine beliebige von ihnen als rationale Funktion mit in $\mathfrak{k}$ enthaltenen Koeffizienten ausdrückbar sind. Bezeichnen

$$(12) \qquad s_0,\ s_1,\ s_2,\ \cdots,\ s_{r-1}$$

die Substitutionen, durch welche dieser Körper $\mathfrak{K}$ in seine relativ konjugierten Körper übergeht, so heißt ihre wieder eine Gruppe bildende Gesamtheit die Relativgruppe, und, wenn die letztere insbesondere eine kommutative oder gar eine zyklische ist, so wird der Körper $\mathfrak{K}$ ein relativ-*Abel*scher bezw. relativ-zyklischer Körper genannt.

2. Nun werde zunächst gezeigt, wie einfach die Idealtheorie des *Galois*schen Körpers begründet werden kann. Es geschieht dies, wie in der allgemeinen Theorie, durch den Beweis des fundamentalen Satzes, daß zu jedem Ideale des Galoisschen Körpers ein anderes bestimmbar ist, so beschaffen, daß beider Produkt ein Hauptideal wird. Hilbert hat in einer bemerkenswerten kleinen Abhandlung[1]) gezeigt, wie solch' Beweis aus dem Begriffe und den einfachsten Eigenschaften des Ideals direkt erbracht werden kann. Wir folgen hier jedoch dem noch einfacheren Gange, den er zu gleichem Zwecke in seinem Bericht über die Theorie der algebraischen Zahlen (Deutsche Math. Verein 4. Bd. S. 248) eingeschlagen hat.

Sei $\mathfrak{J}$ ein Ideal des Galoisschen Körpers $\mathfrak{K}$ vom Grade N. Wir sagen: $\mathfrak{J}$ sei teilbar durch ein anderes Ideal $\mathfrak{J}'$ oder setzen

1) Hilbert, Math. Annalen 44, 1894, p. 1.

$\mathfrak{J} \equiv 0$ (mod. $\mathfrak{J}'$), wenn es in $\mathfrak{J}'$ enthalten ist. Wenn es durch sämtliche Substitutionen der Gruppe des Körpers $\mathfrak{K}$, welche G genannt werde, unverändert, d. h. die Gesamtheit der Zahlen jedes transformierten Ideales von ihrer Anordnung abgesehen mit derjenigen des ursprünglichen identisch bleibt, so heiße $\mathfrak{J}$ ein invariantes Ideal (in der angeführten Abhandlung gebraucht Hilbert statt dessen den Ausdruck „ambiges Ideal"). Für ein solches besteht aber folgender Satz:

Die $N!^{\text{te}}$ Potenz eines invarianten Ideals ist stets gleich einer rationalen ganzen Zahl, in Zeichen:

$$\mathfrak{J}^{N!} = \mathfrak{G}t, \tag{13}$$

wo t eine rationale ganze Zahl und $\mathfrak{G}$ die Gesamtheit der ganzen Zahlen des *Galois*schen Körpers bedeutet. Jede Zahl α des Ideales $\mathfrak{J}$ leistet nämlich einer Gleichung N^{ten} Grades

$$\alpha^N + a_1\alpha^{N-1} + a_2\alpha^{N-2} + \cdots + a_N = 0 \tag{14}$$

mit ganzzahligen Koeffizienten Genüge; daher sind auch die Potenzen

$$a_1^{N!}, \; a_2^{\frac{1}{2}N!}, \; \cdots, \; a_N^{\frac{1}{N}N!} \tag{15}$$

ganze rationale Zahlen, deren größter gemeinsamer Teiler a heiße. In gleicher Weise denke man sich für jede der Zahlen $\alpha, \beta, \gamma, \cdots$ des Ideals die ihnen entsprechenden größten gemeinsamen Teiler $a, b, c, \cdots$ bestimmt, und nenne schließlich wieder t den größten gemeinsamen Teiler aller so bestimmten Zahlen $a, b, c, \cdots$. Dann besteht die Beziehung (13). Um dies einzusehen, bemerke man, daß die zu α konjugierten Zahlen einerseits wieder Zahlen des als invariant vorausgesetzten Ideals $\mathfrak{J}$, andererseits aber die Wurzeln der Gleichung (14) sind, von denen die Koeffizienten dieser Gleichung homogene ganze Funktionen $1^{\text{ter}}, 2^{\text{ter}}, 3^{\text{ter}}, \cdots, N^{\text{ter}}$ Dimension sind. Hieraus folgen die Kongruenzen

$$a_1 \equiv 0 \pmod{\mathfrak{J}}, \quad a_2 \equiv 0 \pmod{\mathfrak{J}^2}, \cdots, a_N \equiv 0 \pmod{\mathfrak{J}^N},$$

denen zufolge wieder die sämtlichen Zahlen (15) in dem Ideale $\mathfrak{J}^{N!}$ enthalten sein müssen. Gleiches gilt daher auch von

ihrem größten gemeinsamen Teiler a, da dieser bekanntlich als eine ganze, ganzzahlige lineare Funktion der Zahlen (15) darstellbar ist. Ebenso müssen aber auch die sämtlichen Zahlen $b, c, \cdots$ und demnach endlich auch t oder, der Definition eines Ideales zufolge, das Hauptideal $\mathfrak{G}t$ in $\mathfrak{J}^{N!}$ enthalten sein. Da andererseits jede der Zahlen (15) durch a also auch durch t teilbar ist, kann man

$$a_i^{\frac{N!}{i}} = t \cdot b_i$$

setzen, wo b_i eine ganze rationale Zahl; daraus folgt

$$a_i = t^{\frac{i}{N!}} \cdot b_i^{\frac{i}{N!}} = t^{\frac{i}{N!}} \cdot c_i$$

wo c_i eine ganze algebraische Zahl ist. Hiernach nimmt die Gleichung (14) die Gestalt an:

$$\alpha^N + c_1 \cdot t^{\frac{1}{N!}} \cdot \alpha^{N-1} + c_2 \cdot t^{\frac{2}{N!}} \cdot \alpha^{N-2} + \cdots + c_N \cdot t^{\frac{N}{N!}} = 0$$

und gibt, wenn $\alpha = t^{\frac{1}{N!}} \cdot \alpha_1$ gesetzt wird, die Gleichung

$$\alpha_1^N + c_1 \alpha_1^{N-1} + c_2 \alpha_1^{N-2} + \cdots + c_N = 0,$$

derzufolge α_1 eine ganze algebraische Zahl ist (s. Kap. 1, Nr. 3). Ebenso ergeben sich für die übrigen Zahlen $\beta, \gamma, \cdots$ des Ideals $\mathfrak{J}$ entsprechende Gleichungen:

$$\beta = t^{\frac{1}{N!}} \cdot \beta_1, \quad \gamma = t^{\frac{1}{N!}} \cdot \gamma_1, \quad \cdots$$

Daher muß aber jede Zahl ζ des Ideals $\mathfrak{J}^{N!}$ von der Form $t \cdot \gamma_0$ sein, wo γ_0 eine ganze algebraische Zahl und zwar als Quotient zweier dem Körper $\mathfrak{K}$ angehöriger Zahlen ζ, t eine ganze Zahl des letztern d. i. der Gesamtheit $\mathfrak{G}$ ist, und so findet sich $\mathfrak{J}^{N!}$ enthalten in $\mathfrak{G}t$. Da auch die umgekehrte Beziehung schon erwiesen ist, erhellt die Richtigkeit der zu beweisenden Gleichung (13).

Auf Grund dieses Satzes erkennt man aber ohne weiteres die Gültigkeit des folgenden: **Zu jedem Ideale $\mathfrak{J}$ des *Galois*schen Körpers gibt es ein anderes $\mathfrak{J}'$ von der Beschaffenheit, daß $\mathfrak{J} \cdot \mathfrak{J}'$ ein Hauptideal wird.**

In der Tat: zugleich mit dem Ideale $\mathfrak{J}$ oder $s_0\mathfrak{J}$ sind auch

$$s_1\mathfrak{J},\ s_2\mathfrak{J},\ \cdots,\ s_{N-1}\mathfrak{J}$$

Ideale des Galoisschen Körpers und ihr Produkt

$$(16)\qquad s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdot s_2\mathfrak{J}\cdots s_{N-1}\mathfrak{J}$$

ist ein invariantes Ideal desselben; denn, wenn man auf dasselbe irgend eine der Substitutionen s_i der Gruppe G anwendet, so bilden die N Substitutionen

$$s_is_0,\ s_is_1,\ s_is_2,\ \cdots,\ s_is_{N-1}$$

wieder die sämtlichen Substitutionen der Gruppe, die Faktoren des Produkts (16) werden also nur vertauscht und das Produkt nicht verändert. Dem voraufgehenden Satze gemäß ist daher die $N!^{\text{te}}$ Potenz dieses Produktes oder der folgende Ausdruck

$$\mathfrak{J}\cdot s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J}\cdot(s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J})^{N!-1}$$

ein Hauptideal, mithin das Ideal

$$\mathfrak{J}'=s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J}\cdot(s_0\mathfrak{J}\cdot s_1\mathfrak{J}\cdots s_{N-1}\mathfrak{J})^{N!-1}$$

ein Ideal von der Art, wie der Satz es behauptet.

3. Nunmehr ließe sich die Arithmetik des Galoisschen Körpers ganz in derselben Weise entwickeln, wie es im sechsten Kapitel für die Zahlenkörper im allgemeinen geschehen ist, und so haben wir nicht nötig, in dieser Richtung weiterzugehen. Dagegen erübrigt noch anzudeuten, wie etwa nun auf Grund dieser besonderen Idealtheorie diejenige eines beliebigen Körpers aufzubauen sein würde. Im Anschluß an Hilberts Abhandlung sei darüber kurz folgendes bemerkt.

Jeder gegebene Körper $\mathfrak{k}$ kann als Unterkörper eines Galoisschen Körpers angesehen werden, z. B. desjenigen, der aus $\mathfrak{k}$ und allen seinen konjugierten Körpern zusammengesetzt ist. Ist aber $\mathfrak{K}$ ein Galoisscher Körper N^{ten} Grades und $\mathfrak{k}$ ein Unterkörper desselben vom Grade n, so wird $\mathfrak{K}$ mit Bezug auf $\mathfrak{k}$ ein Relativkörper r^{ten} Grades sein, wenn $r=\frac{N}{n}$ gesetzt wird, und wird durch die Wurzel A einer Gleichung von der Form (11) erzeugt werden. Die Substitutionen des

Relativkörpers aber, welche diese Wurzel A in ihre relativ Konjugierten, d. i. in die anderen Wurzeln der Gleichung (11) verwandeln, werden diejenigen Substitutionen des ursprünglichen Galoisschen Körpers oder der Gruppe G sein, welche die erzeugende Zahl α des Unterkörpers und somit dessen sämtliche Zahlen ungeändert lassen; wir nennen sie

$$s_0, s_1, s_2, \cdots, s_{r-1}. \tag{17}$$

Sie bilden wieder eine Gruppe, die, weil in der Gesamtgruppe G enthalten, eine Untergruppe von G genannt wird; in der Tat ist ja die Gleichung (11) eine Galoissche, da ihre Wurzeln gewisse Wurzeln der Gleichung (1) sind, welcher der Galoissche Körper $\mathfrak{K}$ entstammt, also rational durch einander ausgedrückt werden können, sodaß die relativ Konjugierten des Relativkörpers mit ihm identisch sind.

Dies vorausgeschickt, sei

$$\mathfrak{j} = \{\alpha_1, \alpha_2, \cdots, \alpha_\mu\}$$

irgend ein Ideal des Unterkörpers $\mathfrak{k}$. Ihm entspricht im Galoisschen Körper $\mathfrak{K}$ ein es in sich enthaltendes Ideal $\mathfrak{J}$, das ihm als gleichbedeutend anzusehen und, wie man leicht erkennt, mit

$$\mathfrak{J} = \mathfrak{G}\mathfrak{j}$$

identisch ist. Nun sei $\mathfrak{H}$ ein Ideal des Galoisschen Körpers, für welches

$$\mathfrak{J} \cdot \mathfrak{H} = \mathfrak{G} \cdot \Omega \tag{18}$$

ein Hauptideal, Ω also eine ganze Zahl des Galoisschen Körpers wird. Hiernach besteht eine Gleichung

$$s_0\Omega = \Omega = \alpha_1 h_1 + \alpha_2 h_2 + \cdots + \alpha_\mu h_\mu,$$

worin die h_i gewisse Zahlen des Ideals $\mathfrak{H}$ bedeuten. Aus ihr aber entstehen durch die Substitutionen der Untergruppe (17) die $r-1$ folgenden:

$$\begin{aligned}
s_1\Omega &= \alpha_1 \cdot s_1 h_1 + \alpha_2 \cdot s_1 h_2 + \cdots + \alpha_\mu \cdot s_1 h_\mu \\
s_2\Omega &= \alpha_1 \cdot s_2 h_1 + \alpha_2 \cdot s_2 h_2 + \cdots + \alpha_\mu \cdot s_2 h_\mu \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
s_{r-1}\Omega &= \alpha_1 \cdot s_{r-1} h_1 + \alpha_2 \cdot s_{r-1} h_2 + \cdots + \alpha_\mu \cdot s_{r-1} h_\mu
\end{aligned}$$

deren Multiplikation mit der vorigen die andere:

$$(19)\qquad \overline{\Omega} = \alpha_1^r \cdot H_1 + \alpha_1^{r-1}\alpha_2 \cdot H_2 + \cdots + \alpha_\mu^r \cdot H_\nu$$

ergibt; hier ist zur Abkürzung

$$\overline{\Omega} = s_0\Omega \cdot s_1\Omega \cdots s_{r-1}\Omega$$

gesetzt, ν bedeutet die Anzahl der aus den $\alpha_1, \alpha_2, \cdots, \alpha_\mu$ möglichen Produkte r^{ter} Dimension, und die H_i sind offenbar aus den Zahlen h_i und ihren Konjugierten symmetrisch zusammengesetzte Ausdrücke, welche durch die Substitutionen der Untergruppe unveränderlich also ganze Zahlen des Körpers $\mathfrak{k}$ sind; dasselbe gilt von der Zahl $\overline{\Omega}$, und zwar ist diese dem Ausdruck (19) zufolge in dem Ideale

$$(20)\qquad \mathfrak{j}^r \cdot \{H_1, H_2, \cdots, H_\nu\}$$

des Körpers $\mathfrak{k}$ enthalten. Andererseits folgt aus (18), daß jede der Zahlen α_i, mit jeder in $\mathfrak{H}$ enthaltenen Zahl, insbesondere also mit jeder der Zahlen h_i multipliziert, durch Ω teilbar ist; deshalb wird jedes Produkt aus r Zahlen α_i in eine der Zahlen H_i zufolge der besonderen Bildung der letzteren eine durch das Produkt $\overline{\Omega}$ teilbare ganze Zahl des Körpers $\mathfrak{k}$ und demnach das Ideal (20) in $\mathfrak{g}\overline{\Omega}$ enthalten sein, wo $\mathfrak{g}$ die Gesamtheit dieser ganzen Zahlen bedeutet. In Verbindung mit dem ersterhaltenen Resultate folgt hieraus die Gleichheit

$$\mathfrak{g}\overline{\Omega} = \mathfrak{j}^r \cdot \{H_1, H_2, \cdots, H_\nu\},$$

d. h. das beliebig gegebene Ideal $\mathfrak{j}$ des Körpers $\mathfrak{k}$ gibt durch Multiplikation mit dem andern Ideale

$$\mathfrak{j}^{r-1} \cdot \{H_1, H_2, \cdots, H_\nu\}$$

desselben eins seiner Hauptideale.

So hat sich durch einfache Überlegungen aus der Theorie des Galoisschen Körpers der fundamentale Satz ergeben, auf dem jetzt die gesamte Arithmetik des Körpers $\mathfrak{k}$, d. i. eines beliebig gegebenen Körpers wieder in früher ausgeführter Weise entwickelt werden kann.

4. Indem wir nun die hauptsächlichsten besonderen Eigenschaften des Galoisschen Körpers darlegen wollen, beginnen wir mit dem Beweise des folgenden Satzes:

Die Differente $\mathfrak{D}$ des *Galois*schen Körpers $\mathfrak{K}$ ist ein invariantes Ideal, und seine Diskriminante D (genauer: das Hauptideal $\mathfrak{G}$D) ist ihre N^{te} Potenz.

Man bezeichne mit

$$\Omega_1, \Omega_2, \cdots, \Omega_N$$

irdend eine Basis des Galoisschen Körpers; seine sogenannten „Elemente", nämlich die Ideale

$$(21)\quad \begin{aligned} \mathfrak{E}^{(1)} &= \{\Omega_1 - s_1\Omega_1,\ \Omega_2 - s_1\Omega_2, \cdots, \Omega_N - s_1\Omega_N\} \\ \mathfrak{E}^{(2)} &= \{\Omega_1 - s_2\Omega_1,\ \Omega_2 - s_2\Omega_2, \cdots, \Omega_N - s_2\Omega_N\} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{E}^{(N-1)} &= \{\Omega_1 - s_{N-1}\Omega_1,\ \Omega_2 - s_{N-1}\Omega_2, \cdots, \Omega_N - s_{N-1}\Omega_N\}, \end{aligned}$$

welche beim allgemeinen Körper diesem selbst nicht anzugehören brauchen, werden hier Ideale des Galoisschen Körpers sein, da die sämtlichen Differenzen in den Ausdrücken (21) Zahlen desselben sind; ihr Produkt aber ist die Differente des Körpers. Wird nun auf die Ideale $\mathfrak{E}^{(1)}, \mathfrak{E}^{(2)}, \cdots, \mathfrak{E}^{(N-1)}$ irgend eine Substitution s_k der Gruppe G angewandt, so geht z. B. $\mathfrak{E}^{(i)}$ über in das Ideal

$$(22)\quad \{s_k\Omega_1 - s_ks_i\Omega_1,\ s_k\Omega_2 - s_ks_i\Omega_2, \cdots, s_k\Omega_N - s_ks_i\Omega_N\},$$

welches zugleich mit seinen Differenzen dem Galoisschen Körper angehört. Da aber zur Substitution s_i immer eine andere:

$$(23)\quad s_{i'} = s_ks_is_k^{-1}$$

vorhanden ist, für welche

$$s_{i'} \cdot s_k = s_ks_i$$

ist, so geht (22) über in den Ausdruck

$$(24)\quad \{s_k\Omega_1 - s_{i'}s_k\Omega_1,\ s_k\Omega_2 - s_{i'}s_k\Omega_2, \cdots, s_k\Omega_N - s_{i'}s_k\Omega_N\},$$

in welchem die Zahlen

$$(25)\quad s_k\Omega_1,\ s_k\Omega_2, \cdots, s_k\Omega_N$$

Basiszahlen eines zu $\mathfrak{K}$ konjugierten, d. i. eben dieses Galoisschen Körpers bezeichnen. Wenn nun s_i alle Substitutionen der Gruppe G durchläuft, so wird gleiches auch mit der durch (23) definierten Substitution $s_{i'}$ geschehen, daher stellen die so

aus (24) hervorgehenden Ideale des Galoisschen Körpers seine der Basis (25) entsprechenden „Elemente“ dar, deren Produkt, eben wie dasjenige der Elemente (21), die von der Wahl der Basiszahlen unabhängige Differente oder das Grundideal des Körpers ausmacht. Dieses letztere verändert sich also nicht bei einer Substitution s_k der Gruppe G oder ist, wie zuvörderst behauptet, ein invariantes Ideal. — Nun ist aber die Grundzahl D des Körpers die Norm seines Grundideales $\mathfrak{D}$; da, wie gezeigt, $s_k\mathfrak{D} = \mathfrak{D}$ ist, findet sich also in der Tat, wie ferner behauptet worden ist,

$$\mathrm{D} = \mathfrak{D}^N. \tag{26}$$

5. Die arithmetischen Eigenschaften des Galoisschen Körpers beruhen, wie seine algebraischen, durchaus auf der Beziehung, in welcher er zu den verschiedenen, in ihm enthaltenen Unterkörpern und diese selbst zu einander stehen. Es ist bereits bemerkt worden, daß die Substitutionen der Gruppe G des Galoisschen Körpers $\mathfrak{K}$, welche die Zahlen eines seiner Unterkörper $\mathfrak{k}$ nicht verändern, selbst wieder eine Gruppe bilden, daß somit zu jedem Unterkörper $\mathfrak{k}$ eine bestimmte Untergruppe g gehört. Das Umgekehrte findet aber offenbar auch statt: zu jeder Untergruppe g gehört ein bestimmter Unterkörper $\mathfrak{k}$ des Galoisschen Körpers, nämlich die Gesamtheit aller Zahlen des letztern, die durch die Substitutionen jener Untergruppe nicht verändert werden, und die offenbar einen Körper bilden. In dieser Weise sind also die Unterkörper des *Galois*schen Körpers und die Untergruppen seiner Gruppe eindeutig einander zugeordnet.

Für die Idealtheorie des Galoisschen Körpers und seiner Unterkörper ist es nun vor allem notwendig, seine Primideale ins Auge zu fassen. Sei also $\mathfrak{P}$ irgend ein Primideal des Körpers $\mathfrak{K}$. Es wird dann stets unter den Substitutionen der Gruppe G eine Anzahl solcher geben, welche, auf $\mathfrak{P}$ angewandt, die Gesamtheit der in $\mathfrak{P}$ enthaltenen Zahlen, von deren Reihenfolge abgesehen, nicht ändern, denn jedenfalls ist die identische Substitution s_0, welche die Zahlen von $\mathfrak{K}$ ungeändert läßt, eine solche. Die gedachten Substitutionen

$$z_0 = s_0, z_1, z_2, \cdots,$$

deren Anzahl r_z heiße, bilden aber, wie leicht ersichtlich, wieder eine Gruppe, welche mit g_z bezeichnet und (nach Hilbert) die Zerlegungsgruppe des Primideals $\mathfrak{P}$ genannt werde. Der dieser Gruppe g_z zugeordnete Unterkörper, d. i. die Gesamtheit aller Zahlen von $\mathfrak{K}$, welche durch ihre Substitutionen unverändert bleiben, heiße der Zerlegungskörper des Primideals $\mathfrak{P}$ und werde mit $\mathfrak{k}_z$ bezeichnet. Sein Grad ist $n_z = \frac{N}{r_z}$; mit bezug auf den Zerlegungskörper ist $\mathfrak{K}$ ein Relativkörper vom Grade r_z.

Der Zerlegungskörper enthält nun in sich einen anderen, welcher von besonderer Wichtigkeit ist. Hilbert, welcher zuerst die Grundzüge einer Arithmetik des Galoisschen Körpers gezeichnet hat (Nachr. der Gött. Ges. 1894 (1895) p. 224; vgl. dazu aber auch Dedekind, ebendas. p. 272, sowie Hilberts Bericht, deutsche Math. Verein. Kap. 10), und dem unsere Darstellung derselben im wesentlichen folgen soll, hat dieser neuen Gruppe den Namen Trägheitsgruppe und dem ihr zugeordneten Unterkörper von $\mathfrak{K}$ den Namen Trägheitskörper des Primideals $\mathfrak{P}$ beigelegt, jene mit g_t, die Anzahl ihrer Substitutionen mit r_t, diesen mit $\mathfrak{k}_t$, seinen Grad $\frac{N}{r_t}$ mit n_t bezeichnet; $\mathfrak{K}$ ist also mit bezug auf den Trägheitskörper ein Relativkörper vom Grade r_t. Die Substitutionen der Trägheitsgruppe aber sind die sämtlichen Substitutionen

$$t_0 = s_0, t_1, t_2, \cdots$$

der Gruppe G, welchen die Eigenschaft zukommt, daß für jede ganze Zahl Ω des Körpers $\mathfrak{K}$

$$t_i\Omega \equiv \Omega \pmod{\mathfrak{P}} \tag{27}$$

ist. Daß diese Substitutionen t_i wirklich eine Gruppe bilden, erkennt man leicht. Denn zunächst ist wegen (27) stets mit Ω zugleich auch $t_i\Omega$ eine Zahl des Ideals $\mathfrak{P}$ und daher das Ideal $t_i\mathfrak{P}$ in $\mathfrak{P}$ enthalten; setzt man aber $\Omega' = t_i^{-1}\Omega$ also $\Omega = t_i\Omega'$, so folgt aus $t_i\Omega' \equiv \Omega' \pmod{\mathfrak{P}}$ die Kongruenz $\Omega \equiv \Omega' \pmod{\mathfrak{P}}$, also ist Ω' zugleich mit Ω in $\mathfrak{P}$ und somit

jede Zahl $\Omega = t_i\Omega'$ des Ideals $\mathfrak{P}$ in $t_i\mathfrak{P}$ enthalten; man erschließt also die Gleichheit $t_i\mathfrak{P} = \mathfrak{P}$ und daß daher die Substitutionen t_i zu denjenigen zählen, welche das Primideal $\mathfrak{P}$ nicht verändern. Aus diesem Grunde folgt aber aus (27) durch Anwendung einer andern Substitution t_k derselben Art wie t_i die Kongruenz

$$t_k t_i \Omega \equiv t_k \Omega \pmod{\mathfrak{P}},$$

d. h. mit Rücksicht auf die vorausgesetzte Kongruenz

$$t_k \Omega \equiv \Omega \pmod{\mathfrak{P}}$$

diese andere:

$$t_k t_i \Omega \equiv \Omega \pmod{\mathfrak{P}};$$

demnach ist, was zu zeigen war, das Produkt zweier der Substitutionen t_i wieder eine derselben, und ihre Gesamtheit eine Gruppe. Die Trägheitsgruppe ist zudem nach dem Bemerkten eine Untergruppe der Zerlegungsgruppe und sonach der Zerlegungskörper im Trägheitskörper enthalten.

6. Um das Verhältnis beider Gruppen zu einander klarer zu stellen, sei jetzt p die dem Primideale $\mathfrak{P}$ charakteristische, d. h. in ihm enthaltene Primzahl und f sein Grad, so daß die Gleichung stattfindet:

$$\mathfrak{N}(\mathfrak{P}) = p^f$$

oder, wie man sie nach Kap. 11, Nr. 1 auch schreiben darf,

$$N(\mathfrak{P}) = p^f. \tag{28}$$

Wir beweisen dann zuerst, daß es eine, wenn $f > 1$, nicht in der Trägheitsgruppe enthaltene Substitution z der Zerlegungsgruppe gibt von der Beschaffenheit, daß z^f der Trägheitsgruppe angehört, daß nämlich für jede ganze Zahl Ω in $\mathfrak{K}$

$$z^f \Omega \equiv \Omega \pmod{\mathfrak{P}} \tag{29}$$

ist. Zu diesem Zwecke wählen wir eine Primitivzahl P (mod. $\mathfrak{P}$), die wir offenbar (vgl. Kap. 6, Nr. 15) der besonderen Bedingung unterwerfen können, daß sie durch alle zu $\mathfrak{P}$ konjugierten, doch von $\mathfrak{P}$ verschiedenen Primideale, die im Galoisschen Körper Primidealfaktoren von p sind, teilbar sei. Eine solche

Zahl genügt, wie jede Zahl des Galoisschen Körpers einer ganzzahligen Gleichung N^{ten} Grades $\psi(x) = 0$, deren übrige Wurzeln ihre Konjugierten sind, sodaß man setzen darf

$$(30) \qquad \psi(x) = (x - s_0\mathrm{P})(x - s_1\mathrm{P}) \cdots (x - s_{N-1}\mathrm{P}) = 0.$$

Faßt man diese Gleichung aber als eine Kongruenz (mod. $\mathfrak{P}$), so hat sie nach Kap. 6, Nr. 21 zugleich mit der Wurzel P auch die Wurzel P^p und demnach muß es eine Substitution s_i der Gruppe G geben, für welche

$$(31) \qquad s_i\mathrm{P} \equiv \mathrm{P}^p \pmod{\mathfrak{P}}$$

ist. Diese Substitution gehört aber der Zerlegungsgruppe an; denn, wäre nicht $s_i\mathfrak{P} = \mathfrak{P}$, also auch nicht $s_i^{-1}\mathfrak{P} = \mathfrak{P}$, so wäre $s_i^{-1}\mathfrak{P}$ mit einem der zu $\mathfrak{P}$ konjugierten, aber von $\mathfrak{P}$ verschiedenen Ideale identisch und, da nach der Voraussetzung P durch diese letzteren teilbar ist, wäre $s_i\mathrm{P}$ teilbar durch $\mathfrak{P}$, was die Kongruenz (31) nicht zuläßt. Setzt man hiernach für s_i das Zeichen z, sodaß

$$(32) \qquad z\mathrm{P} \equiv \mathrm{P}^p \pmod{\mathfrak{P}}$$

ist, so folgert man hieraus die weiteren Kongruenzen:

$$z^2\mathrm{P} \equiv \mathrm{P}^{p^2}, \quad z^3\mathrm{P} \equiv \mathrm{P}^{p^3}, \cdots, z^f\mathrm{P} \equiv \mathrm{P}^{p^f} \pmod{\mathfrak{P}}$$

und, da die Primitivzahl P (Kap. 6, Nr. 22) zum Exponenten f paßt, kommt der Substitution z die Eigenschaft zu, daß f die kleinste positive ganze Zahl ist, für welche

$$(33) \qquad z^f\mathrm{P} \equiv \mathrm{P} \pmod{\mathfrak{P}}$$

wird, woraus hervorgeht, daß, wenn $f > 1$, die Substitution z keine Substitution der Trägheitsgruppe ist. Nun ist aber jede ganze Zahl Ω des Galoisschen Körpers entweder teilbar durch $\mathfrak{P}$, oder einer Potenz P^i (mod. $\mathfrak{P}$) kongruent. Im ersteren Falle ist sicherlich schon, weil z zur Zerlegungsgruppe gehört, $z\Omega \equiv \Omega$ also auch $z^f\Omega \equiv \Omega$ (mod. $\mathfrak{P}$); im andern Falle folgt aus

$$\Omega \equiv \mathrm{P}^i \pmod{\mathfrak{P}}$$

mit Rücksicht auf (33) die Kongruenz

$$z^f\,\Omega \equiv z^f(\mathrm{P}^i) \equiv (z^f\mathrm{P})^i \equiv \mathrm{P}^i \equiv \Omega \pmod{\mathfrak{P}}.$$

Mithin hat die angegebene Substitution z die zu Beweis stehende Eigenschaft, und zwar ist mit Beachtung des von der Kongruenz (33) Gesagten f die niedrigste Zahl, für welche die Kongruenz (29) für jede ganze Zahl des Galoisschen Körpers erfüllt wird.

Nunmehr sieht man zweitens leicht ein, daß die gesamte Zerlegungsgruppe in die folgenden f Komplexe von Substitutionen, in denen jedesmal t die sämtlichen Substitutionen der Trägheitsgruppe bezeichnet, zerfällt:

$$(34) \qquad t,\ z\cdot t,\ z^2\cdot t,\ \cdots,\ z^{f-1}\cdot t$$

oder daß, nach einer Schreibweise von *Galois*, die gesamte Gruppe

$$(35) \qquad g_z = g_t + z\cdot g_t + \cdots + z^{f-1}\cdot g_t$$

ist. Die Primitivzahl P leistet nämlich nach Kap. 6, Nr. 21 und 22 einer irreduktibeln ganzzahligen Kongruenz f^{ten} Grades (mod. $\mathfrak{P}$) Genüge, welche

$$P(x) \equiv 0 \pmod{\mathfrak{P}}$$

heiße, und welche genau f Wurzeln hat, nämlich die f Potenzen $\mathrm{P},\ \mathrm{P}^p,\ \cdots,\ \mathrm{P}^{p^{f-1}}$; es ist also insbesondere

$$P(\mathrm{P}) \equiv 0 \pmod{\mathfrak{P}}.$$

Durch Anwendung irgend einer Substitution z_i der Zerlegungsgruppe folgt hieraus

$$P(z_i\mathrm{P}) \equiv 0 \pmod{\mathfrak{P}}$$

und somit, wenn k eine der Zahlen $0, 1, 2, \cdots, f-1$ bedeutet,

$$z_i\mathrm{P} \equiv \mathrm{P}^{p^k} \equiv z^k\mathrm{P}$$

d. h. $z^{-k}z_i\mathrm{P} \equiv \mathrm{P} \pmod{\mathfrak{P}}$, woraus sich leicht, wie oben, wieder

$$z^{-k}z_i\Omega \equiv \Omega \pmod{\mathfrak{P}}$$

für jede ganze Zahl Ω des Galoisschen Körpers herausstellt. Also ist $z^{-k}z_i$ eine Substitution t der Trägheitsgruppe und jede Substitution z_i der Zerlegungsgruppe von der Form

$$z_i = z^k\cdot t$$

d. h. in einem der Komplexe (34) enthalten. Diese bestehen aber ihrerseits auch nur aus Substitutionen der Zerlegungsgruppe, und daß die verschiedenen Komplexe auch aus verschiedenen solcher Substitutionen gebildet sind, leuchtet unmittelbar daraus ein, daß z^f die niedrigste Potenz der Substition z mit positivem Exponenten ist, die zu den Substitutionen t gehört. Die Komplexe (34) machen demnach in der Tat die gesamte Zerlegungsgruppe aus.

Aus (32) folgt

$$t_i z \mathrm{P} \equiv t_i \mathrm{P}^p \pmod{\mathfrak{P}}$$

für jede Substitution t_i der Trägheitsgruppe; da nun nach der Natur dieser Substitutionen

$$t_i \mathrm{P}^p \equiv \mathrm{P}^p \pmod{\mathfrak{P}}$$

ist, findet sich mit Rücksicht auf (32)

$$t_i z \mathrm{P} \equiv z \mathrm{P}$$

und folglich

$$z^{-1} t_i z \mathrm{P} \equiv \mathrm{P} \pmod{\mathfrak{P}},$$

eine Kongruenz, aus welcher wieder allgemeiner für jede ganze Zahl Ω des Galoisschen Körpers

$$z^{-1} t_i z \Omega \equiv \Omega \pmod{\mathfrak{P}}$$

erschlossen wird. Somit gehört die Substitution $z^{-1} t_i z$ der Trägheitsgruppe an. Diese Gruppe hat demnach die Eigenschaft, welche durch die Beziehung

$$z^{-1} \cdot g_t \cdot z = g_t \tag{36}$$

ausgedrückt werden kann und als „Invarianz" der Trägheitsgruppe bezeichnet wird.

Aus (35) geht unschwer hervor, daß in vorstehender Formel die Substitution z durch eine beliebige Substitution s_i der Zerlegungsgruppe ersetzt werden kann.

Es ist nunmehr leicht, zunächst das Gesetz anzugeben, nach welchem die Primzahl p im Galoisschen Körper in Primidealfaktoren zerfällt. Da g_z eine Untergruppe der Gesamtgruppe G dieses Körpers und r_z ihr Grad, d. i. die Anzahl ihrer Substitutionen ist, so gibt es in G gewisse Substitutionen $s_0, s_1, \cdots, s_{n_z - 1}$, so beschaffen, daß die gesamte Gruppe G in die Komplexe

(37) $$s_0 \cdot g_z,\ s_1 \cdot g_z,\ \cdots,\ s_{n_z-1} \cdot g_z$$

zerfällt, oder daß

(38) $$G = s_0 \cdot g_z + s_1 \cdot g_z + \cdots + s_{n_z-1} \cdot g_z$$

gesetzt werden kann. Wendet man nun, um alle N Konjugierten des Primideals $\mathfrak{P}$ zu erhalten, auf dasselbe alle Substitutionen der Gruppe G an, so liefert jeder der Komplexe (37) je eins der Primideale

(39) $$s_0\mathfrak{P} = \mathfrak{P},\ s_1\mathfrak{P},\ \cdots,\ s_{n_z-1}\mathfrak{P},$$

welche notwendig auch voneinander verschieden sind; denn, wäre etwa $s_1\mathfrak{P} = s_2\mathfrak{P}$, so folgte $s_1^{-1}s_2\mathfrak{P} = \mathfrak{P}$, folglich wäre $s_1^{-1}s_2$ eine Substitution z_i der Zerlegungsgruppe, also $s_2 = s_1 z_i$, d. h. gleich einer Substitution des Komplexes $s_1 \cdot g_z$, was der Aufstellung dieser Komplexe widerspricht. Jedes der Primideale (39) entsteht aber bei Anwendung der Substitutionen der Gruppe G auf $\mathfrak{P}$ gleich oft, nämlich so oft, als der entsprechende Komplex Substitutionen umfaßt, d. i. r_z mal. Mit Rücksicht hierauf liefert die Formel (28) die Beziehung

$$p^f = (\mathfrak{P} \cdot s_1\mathfrak{P} \cdot s_2\mathfrak{P} \cdots s_{n_z-1}\mathfrak{P})^{r_z}.$$

Da aber aus der Formel (35) sich

(40) $$r_z = f \cdot r_t$$

ergibt, so nimmt diese Beziehung die einfachere Form an:

(41) $$p = (\mathfrak{P} \cdot s_1\mathfrak{P} \cdot s_2\mathfrak{P} \cdots s_{n_z-1}\mathfrak{P})^{r_t}$$

und liefert das gesuchte Gesetz für die Zerfällung der Primzahl p in ihre Primidealfaktoren im Galoisschen Körper $\mathfrak{K}$.

7. Das Nächste ist nun, hieraus die Primidealfaktoren herzuleiten, in welche dieselbe Primzahl p in irgend einem Unterkörper $\mathfrak{k}$ von $\mathfrak{K}$ sich zerlegt. Ist n der Grad von $\mathfrak{k}$, so gehört $\mathfrak{k}$ zu einer Untergruppe g von G, welche $r = \frac{N}{n}$ Substitutionen enthält, diejenigen nämlich, welche die Zahlen in $\mathfrak{k}$ nicht verändern (s. Nr. 3). Um unser Ziel zu erreichen, müssen wir auf die Beziehungen eingehen, welche diese Untergruppe g mit der Zerlegungs- und der Trägheitsgruppe verbinden.

Sei s eine Substitution in G, z' jede Substitution der Zerlegungsgruppe, s' jede Substitution der Gruppe g, so bilden die sämtlichen Substitutionen von der Form $s' s z'$ einen Komplex, den wir

$$g \cdot s \cdot g_z \tag{42}$$

nennen können. Die $r \cdot r_z$ darin enthaltenen Substitutionen sind aber nicht sämtlich verschieden. Um dies zu übersehen, setzen wir

$$s' s z' = s'' s z'' \tag{43}$$

voraus, indem wir auch unter s'', z'' Substitutionen in g und g_z resp. verstehen; daraus ergibt sich

$$s''^{-1} \cdot s' = s(z'' z'^{-1}) s^{-1}.$$

Nun sind $s''^{-1} s'$ und $z'' z'^{-1}$ Substitutionen s^0, z^0 in g und g_z resp.; demnach werden die zwei Substitutionen (43) des Komplexes dann und nur dann einander gleich sein, wenn

$$s^0 = s \cdot z^0 \cdot s^{-1} \tag{44}$$

d. h. wenn diese auf doppelte Weise ausgedrückte Substitution den beiden Gruppen g und $s \cdot g_z \cdot s^{-1}$ gemeinsam ist. Die Substitutionen aber, welche zweien Gruppen gemeinsam sind, bilden stets wieder eine Gruppe, die hier mit γ bezeichnet werde, während ihr Grad h heiße. Ist also $s' s z'$ eine Substitution des Komplexes (42), so entspricht jeder der h Substitutionen (44) der Gruppe γ eine bestimmte andere Substitution $s'' s z''$ desselben Komplexes, die jener gleich ist, bei welcher nämlich s'', z'' durch die Gleichungen

$$s''^{-1} s' = s^0, \quad z'' z'^{-1} = z^0$$

bestimmt sind. Demnach werden immer je h der Substitutionen des Komplexes (42) einander gleich und deshalb $r \cdot r_z$ ein Vielfaches von h sein.

Man kann nun sämtliche Substitutionen der Gruppe G in eine Anzahl Komplexe von der Form (42) verteilen, indem man für s verschiedene Substitutionen setzt, die wegen (38) nur aus der Reihe

$$s_0, s_1, s_2, \cdots, s_{n_z - 1} \tag{45}$$

gewählt zu werden brauchen. Sind nämlich s_i, s_k zwei solche Substitutionen, so werden die entsprechenden Komplexe

$$g \cdot s_i \cdot g_z, \quad g \cdot s_k \cdot g_z,$$

welche ausschließlich aus Substitutionen der Gruppe G bestehen, die gleichen oder durchweg verschiedene Substitutionen enthalten, je nachdem s_k dem ersteren Komplexe angehört oder nicht, denn im ersten Falle ist $s_k = s' s_i z'$ also

$$g \cdot s_k \cdot g_z = g s' \cdot s_i \cdot z' g_z,$$

wo nun die Substitutionen von den Formen gs', $z'g_z$ mit den Gruppen g, g_z resp. identisch sind; im zweiten Falle kann eine Gleichheit

$$s' s_i z' = s'' s_k z''$$

nicht bestehen, da aus ihr sich die andere:

$$s_k = s''^{-1} s' \cdot s_i \cdot z' z''^{-1},$$

d. h. s_k sich gegen die Voraussetzung als eine Zahl des ersteren Komplexes ergäbe. Hiernach erhält man sämtliche Substitutionen der Gruppe G, wenn man für eine gewisse Anzahl e Substitutionen der Reihe (45) — wir nennen sie

$$s_0, s_1, s_2, \cdots, s_{e-1}$$

— die Komplexe

$$g \cdot s_0 \cdot g_z, \; g \cdot s_1 \cdot g_z, \; \cdots, \; g \cdot s_{e-1} \cdot g_z \tag{46}$$

von der Form (42) bildet; jedoch wird so die Substitution der Gruppe G, je nachdem sie in dem ersten, zweiten, usw. dieser Komplexe sich findet, bezw.

$$h_0, h_1, \cdots, h_{e-1}$$

Mal auftreten, wenn h_i den Grad der Gruppe γ_i bezeichnet, welche die den Gruppen g und

$$g_z^{(i)} = s_i \cdot g_z \cdot s_i^{-1} \tag{47}$$

gemeinsamen Substitutionen enthält.

Man bemerke endlich, daß, weil γ_i eine Untergruppe von g ist, die letztere in eine gewisse Anzahl e_i von Komplexen zerfällt von der Form

$$s' \cdot \gamma_i, \; s'' \cdot \gamma_i, \; \cdots, \; s^{(e_i)} \cdot \gamma_i, \tag{48}$$

wo $s' = s_0, s'', \cdots, s^{(e_i)}$ Substitutionen in g bedeuten, oder daß

(49) $$g = s' \cdot \gamma_i + s'' \cdot \gamma_i + \cdots + s^{(e_i)} \cdot \gamma_i$$

gesetzt werden kann. Man entnimmt hieraus die Gleichung

(50) $$r = h_i \cdot e_i.$$

8. Die festgestellten Umstände genügen nun, um alles herzuleiten, was für die Zerlegung der Primzahl p in Primidealfaktoren des Unterkörpers $\mathfrak{k}$ wesentlich ist. Zu diesem Zwecke sei wieder $\mathfrak{P}$ einer der Primidealfaktoren von p im Körper $\mathfrak{K}$. Dies Ideal hat mit dem Unterkörper $\mathfrak{k}$ gewisse Zahlen gemeinsam, wie denn insbesondere die Primzahl p eine solche ist; die Gesamtheit $\mathfrak{p}$ aller dieser Zahlen aber ist ein Primidealfaktor von p in $\mathfrak{k}$. In der Tat ist offenbar zunächst $\mathfrak{p}$ ein Ideal in $\mathfrak{k}$ (s. Kap. 11, Nr. 1 das über das Ideal J Gesagte). Zudem ist $\mathfrak{G}\mathfrak{p}$ ein in $\mathfrak{P}$ enthaltenes Ideal des Körpers $\mathfrak{K}$, mithin $\mathfrak{P}$ ein Primidealfaktor von $\mathfrak{p}$. Endlich ist aber auch $\mathfrak{p}$ ein *Primideal* des Unterkörpers $\mathfrak{k}$, denn wäre $\mathfrak{p} = \mathfrak{q} \cdot \mathfrak{r}$, wo auch $\mathfrak{q}$, $\mathfrak{r}$ Ideale in $\mathfrak{k}$, also $\mathfrak{G}\mathfrak{q}$, $\mathfrak{G}\mathfrak{r}$ Ideale in $\mathfrak{K}$ bezeichnen, so müßte, da $\mathfrak{p}$ oder $\mathfrak{G}\mathfrak{p}$ in $\mathfrak{P}$ enthalten ist, auch einer der Faktoren $\mathfrak{G}\mathfrak{q}$, $\mathfrak{G}\mathfrak{r}$ es sein und folglich etwa $\mathfrak{q}$ in $\mathfrak{p}$ enthalten sein, während doch auch umgekehrt $\mathfrak{p}$ als durch $\mathfrak{q}$ teilbar in $\mathfrak{q}$ enthalten ist, mithin ergäbe sich $\mathfrak{q} = \mathfrak{p}$ und $\mathfrak{r} = \mathfrak{g}$, was nicht angenommen wird.

Jedem Primidealfaktor $\mathfrak{P}$ von p in $\mathfrak{K}$ entspricht also ein durch denselben teilbarer Primidealfaktor $\mathfrak{p}$ von p in $\mathfrak{k}$.

Umgekehrt entspricht jedem Primidealfaktor $\mathfrak{p}$ von p in $\mathfrak{k}$ ein Ideal $\mathfrak{G}\mathfrak{p}$ in $\mathfrak{K}$, welches zwar kein Primideal zu sein braucht, aber, da es die Primzahl p in sich enthält, ein Idealteiler von p ist und daher durch mindestens einen Primidealfaktor $\mathfrak{P}$ von p in $\mathfrak{K}$ aufgeht. Für einen jeden solchen ist zudem $\mathfrak{p}$ die Gesamtheit der Zahlen, welche $\mathfrak{P}$ mit $\mathfrak{k}$ gemeinsam hat; denn, wäre $\mathfrak{p}$ von der Gesamtheit $\mathfrak{p}'$ dieser Zahlen, welche, wie zuvor bewiesen, ein durch $\mathfrak{P}$ teilbarer Primidealfaktor von p in $\mathfrak{k}$ ist, verschieden, so müßte $\mathfrak{p}$, da es in $\mathfrak{G}\mathfrak{p}$ also auch in $\mathfrak{P}$ und folglich in $\mathfrak{p}'$ enthalten ist, durch $\mathfrak{p}'$ teilbar sein, was doch nur sein kann, wenn die Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ in $\mathfrak{k}$ identisch sind.

Somit gibt es zu jedem Primidealfaktor $\mathfrak{p}$ von p

in $\mathfrak{k}$ mindestens einen Primidealfaktor $\mathfrak{P}$ von p in $\mathfrak{K}$, in welchem $\mathfrak{p}$ als die Gesamtheit der $\mathfrak{k}$ und $\mathfrak{P}$ gemeinsamen Zahlen enthalten ist.

Man wird demnach sämtliche Primidealfaktoren $\mathfrak{p}$ von p in $\mathfrak{k}$ und nur solche finden, wenn man für alle Primidealfaktoren $\mathfrak{P}$ von p in $\mathfrak{K}$ deren größten mit $\mathfrak{k}$ gemeinsamen Teil ermittelt. Nun sind, wenn $\mathfrak{P}$ ein beliebiges in p aufgehendes Primideal in $\mathfrak{K}$ bedeutet, $s_0\mathfrak{P}$, $s_1\mathfrak{P}$, $\cdots$, $s_{N-1}\mathfrak{P}$ die sämtlichen Primfaktoren von p in $\mathfrak{K}$. Betrachtet man von ihnen diejenigen, welche den Substitutionen des Komplexes

$$g \cdot s_i \cdot g_z = g \cdot s_i g_z s_i^{-1} \cdot s_i$$

entsprechen, und bedenkt, daß, wie die Gruppe g_z die Gesamtheit der Substitutionen bezeichnet, welche $\mathfrak{P}_0 = s_0\mathfrak{P} = \mathfrak{P}$ nicht verändern, gleicherweise die Gruppe

$$g_z^{(i)} = s_i g_z s_i^{-1}$$

die Gesamtheit derjenigen Substitutionen ist, durch welche $\mathfrak{P}_i = s_i\mathfrak{P}$ sich nicht verändert, daß dagegen die Substitutionen der Gruppe g zugleich mit dem Körper $\mathfrak{k}$ auch sein Ideal $\mathfrak{p}$ nicht ändern, so leuchtet ein, daß die $\frac{r \cdot r_z}{h_i}$ verschiedenen Substitutionen des Komplexes $g \cdot s_i \cdot g_z$ nur einen und denselben Primidealfaktor $\mathfrak{p}_i$ von p in $\mathfrak{k}$ liefern, und man schließt daher zuvörderst, daß es nicht mehr als e verschiedene Primidealfaktoren

$$\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{e-1}$$

von p in $\mathfrak{k}$ geben kann.

Dieser Herleitung gemäß ist $\mathfrak{p}_i$ durch jeden der Primidealfaktoren $s\mathfrak{P}$ von p, welche den Substitutionen s des Komplexes gs_ig_z entsprechen, teilbar; man darf aber hinzusetzen: auch nur durch sie. Zum Beweise hiervon sei $\mathfrak{P}'$ ein von jenen Primidealfaktoren verschiedener Primteiler von p im Körper $\mathfrak{K}$, und ζ eine Zahl dieses Körpers, welche durch das Produkt jener Primidealfaktoren $s\mathfrak{P}$ teilbar, übrigens aber prim gegen p ist, sodaß

$$\zeta = \Pi s\mathfrak{P} \cdot \mathfrak{Q}$$

gesetzt werden kann, wo die Multiplikation auf alle Substitutionen des Komplexes zu beziehen ist und $\mathfrak{Q}$ ein zu p primes

Ideal in $\mathfrak{K}$ bedeutet (nach dem Satze in Kap. 6, Nr. 17, Anfang, gibt es eine solche Zahl ζ). Bezeichnet nun σ irgend eine Substitution in g, so wird die Anwendung derselben auf ζ das Produkt $\Pi s \mathfrak{P}$ ungeändert lassen, während das konjugierte Ideal $\sigma\mathfrak{Q}$ prim zu p bleibt. Das Produkt dieser Werte $\sigma\zeta$, d. h. die Relativnorm der Zahl ζ in bezug auf den Körper $\mathfrak{k}$ wird mithin eine Zahl dieses Körpers sein, welche durch $\Pi s \mathfrak{P}$, insbesondere also durch $\mathfrak{P}_i$ teilbar, mithin in $\mathfrak{p}_i$ enthalten, andererseits aber durch $\mathfrak{P}'$ nicht teilbar ist; demnach kann auch $\mathfrak{p}_i$ nicht durch $\mathfrak{P}'$ teilbar sein. — Um nun die verschiedenen Primteiler von $\mathfrak{p}_i$ zu ermitteln, erinnern wir uns der Formel (49), in welcher γ_i die Gruppe derjenigen Substitutionen bedeutet, welche den Gruppen g und $g_z^{(i)}$ gemeinsam sind und daher weder das Primideal $\mathfrak{p}_i$ noch $\mathfrak{P}_i$ verändern. Nach dieser Gleichung kann man setzen

$$g s_i g_z = g \cdot g_z^{(i)} \cdot s_i = \sum_{k=1}^{e_i} s^{(k)} \cdot g_z^{(i)} s_i,$$

und hieraus leuchtet ein, daß nur genau e_i Primideale $\mathfrak{P}$ vorhanden sind, nämlich die Ideale

$$\mathfrak{P}_{i,k} = s^{(k)} \mathfrak{P}_i \qquad (\text{für } k = 1, 2, \cdots, e_i),$$

welche dem Primidealfaktor $\mathfrak{p}_i$ entsprechen d. h. Primteiler desselben in $\mathfrak{K}$ sind. So erhält man

$$e_0 + e_1 + \cdots + e_{s-1}$$

Primidealfaktoren

$$(52) \qquad \begin{cases} \mathfrak{P}_{01}, & \mathfrak{P}_{02}, & \cdots, \mathfrak{P}_{0,e_0} \\ \mathfrak{P}_{11}, & \mathfrak{P}_{12}, & \cdots, \mathfrak{P}_{1,e_1} \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ \mathfrak{P}_{s-1,1}, & \mathfrak{P}_{s-1,2}, & \cdots, \mathfrak{P}_{s-1,e_{s-1}}, \end{cases}$$

die je die in $\mathfrak{p}_0, \mathfrak{p}_1, \cdots, \mathfrak{p}_{s-1}$ aufgehenden Primfaktoren sind und alle verschiedenen Primidealfaktoren von p in $\mathfrak{K}$ umfassen müssen; da jedoch der Komplex $g s_i g_z$ eine Anzahl $\frac{r \cdot r_z}{h_i} = r_z \cdot e_i$, die Gesamtgruppe G aber $r_z \cdot n_z$ verschiedene Substitutionen enthält, so ergibt sich die Gleichung

$$r_z(e_0 + e_1 + \cdots + e_{s-1}) = r_z \cdot n_z$$

oder

$$e_0 + e_1 + \cdots + e_{s-1} = n_z,$$

d. h. die Primideale (52) sind die Gesamtheit aller verschiedenen Primidealfaktoren von p in $\mathfrak{K}$ und die e Primideale $\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{e-1}$ sind daher in der Tat voneinander verschieden.

Um ihre Zusammensetzung aus den, einem jeden von ihnen entsprechenden der Ideale (52) zu finden, sei $\mathfrak{P}_{i1}^{x_i}$ die höchste Potenz von $\mathfrak{P}_{i1}$, welche in $\mathfrak{p}_i$ aufgeht, sodaß $\mathfrak{p}_i$ oder genauer

$$\mathfrak{S}\mathfrak{p}_i = \mathfrak{P}_{i1}^{x_i} \cdot \mathfrak{Q}$$

gesetzt werden kann, wo $\mathfrak{Q}$ ein nicht mehr durch $\mathfrak{P}_{i1}$ teilbares Ideal in $\mathfrak{K}$ bedeutet. Durch die Substitutionen s', s'', $\cdots$, $s^{(e_i)}$ ergibt sich dann offenbar, daß $\mathfrak{S}\mathfrak{p}_i$ auch genau durch jede der Potenzen $\mathfrak{P}_{ik}^{x_i}$ $(k = 2, 3, \cdots, e_i)$ teilbar, also

$$\mathfrak{S}\mathfrak{p}_i = (\mathfrak{P}_{i1} \cdot \mathfrak{P}_{i2} \cdots \mathfrak{P}_{i, e_i})^{x_i} \tag{53}$$

sein wird, wo nur noch der Wert des Exponenten x_i zu bestimmen bleibt. Zu diesem Zwecke bedenke man, daß p oder genauer $\mathfrak{S}p$ den Primfaktor $\mathfrak{P}_i = \mathfrak{P}_{i1}$ genau in der Potenz $\mathfrak{P}_{i1}^{r_i}$, oder, was dafür gesetzt werden kann, das Produkt

$$\Pi s \mathfrak{P}_i \tag{53^a}$$

enthält, in welchem die Multiplikation auf die sämtlichen r_i Substitutionen auszudehnen ist, welche $\mathfrak{P}_i$ nicht verändern, d. i. auf die Substitutionen von der Form $s_i t s_i^{-1}$. Aber nur diejenigen Faktoren $s\mathfrak{P}_i$ dieses Produktes sind Primidealfaktoren von $\mathfrak{p}_i$, bei denen s auch zugleich eine Substitution der Gruppe g ist, die übrigen entfallen auf die Konjugierten von $\mathfrak{p}_i$. Jene, den Gruppen

$$g_i^{(i)} = s_i \cdot g_i \cdot s_i^{-1}$$

und g gemeinsamen Substitutionen s bilden eine Untergruppe der erstgenannten, welche $\gamma_i^{(i)}$ heiße; ihr Grad t_i, d. i. die Anzahl ihrer Substitutionen ist ein Teiler von r_i oder

$$r_i = t_i \cdot d_i, \tag{54}$$

und genau t_i Faktoren des Produkts (53ᵃ) enthalten auch das Primideal $\mathfrak{p}_i$, welches daher durch den Primidealfaktor $\mathfrak{P}_i = \mathfrak{P}_{i1}$ genau t_i Mal teilbar ist. Demnach ist $x_i = t_i$ und man hat die Formel:

$$\mathfrak{S}\mathfrak{p}_i = (\mathfrak{P}_{i1} \cdot \mathfrak{P}_{i2} \cdots \mathfrak{P}_{i, e_i})^{t_i}, \tag{55}$$

durch welche die Zerlegung des Primideals $\mathfrak{p}_i$ in Primidealfaktoren in $\mathfrak{K}$ geleistet wird. Da aber p oder $\mathfrak{G}p$ den Primidealfaktor $\mathfrak{P}_{i1}$ genau r_i Mal enthält, findet sich weiter für die Zerlegung von p in Primidealfaktoren des Körpers $\mathfrak{k}$ die folgende Gleichung: p oder

$$(56) \qquad \mathfrak{g}p = \mathfrak{p}_0^{d_0}\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_{\varrho-1}^{d_{\varrho-1}}.$$

Ist hiermit die Zerlegung von p im Unterkörper $\mathfrak{k}$ zwar erledigt, so bleibt doch noch übrig, die Grade seiner Primidealfaktoren $\mathfrak{p}_i$ zu bestimmen. Heißt f_i der Grad von $\mathfrak{p}_i$, so ist zu setzen

$$(57) \qquad p^{f_i} = n(\mathfrak{p}_i),$$

wo mit $n(\mathfrak{p}_i)$ die im Körper $\mathfrak{k}$ genommene Norm des Primideals $\mathfrak{p}_i$ bezeichnet ist. Die letztere ist aber das Produkt der zu $\mathfrak{p}_i$ Konjugierten, welche man erhält, indem man auf $\mathfrak{p}_i$ n Substitutionen s der Gesamtgruppe G anwendet, welche $\mathfrak{k}$ in seine Konjugierten verwandelt. Bringt man statt dessen sämtliche Substitutionen der Gruppe G zur Anwendung, so entsteht jedes der mit einander konjugierten Primideale genau r Mal und demnach wird

$$(58) \qquad p^{rf_i} = \Pi s\mathfrak{p}_i$$

sein, die Multiplikation auf sämtliche Substitutionen der Gruppe G ausgedehnt. Die letzteren werden aber auch durch die Komplexe (46) gegeben, wobei jedoch allgemein die Substitutionen des Komplexes $g \cdot s_i \cdot g_z$ zu je h_i einander gleich sind. Nun sind die Substitutionen s dieses Komplexes und sie allein diejenigen, welche das Primideal $\mathfrak{p}_i$ bestimmen, mithin die $\frac{r \cdot r_z}{h_i} = e_i r_z$ Substitutionen des Komplexes $g \cdot g_z^{(i)}$ diejenigen Substitutionen der Gruppe G, für welche $s\mathfrak{p}_i = \mathfrak{p}_i$ ist. Demnach findet sich unter den Faktoren $s\mathfrak{p}_i$ des Produkts (58) der Primidealfaktor $\mathfrak{p}_i$ genau $e_i r_z$ Mal vor. Da er aber nach (56) in der Potenz p^{rf_i} genau $d_i r f_i$ Mal vorhanden ist, so ergibt sich die Beziehung

$$(59) \qquad d_i r f_i = e_i r_z.$$

Nun ist, weil die Gruppe $g_t^{(i)} = s_i g_t s_i^{-1}$ ein Teiler der Gruppe $g_z^{(i)} = s_i g_z s_i^{-1}$ ist, offenbar auch die Gruppe $\gamma_t^{(i)}$ der Substitutionen, welche g mit der ersteren gemeinsam hat, ein Teiler

der Gruppe γ_i, d. i. der Gesamtheit der Substitutionen, die g und der zweiten Gruppe gemeinsam sind; demnach ist t_i ein Teiler von h_i und es kann

$$(60) \qquad h_i = t_i u_i$$

gesetzt werden. Man erkennt ferner, analog wie bei (42), daß der Substitutionenkomplex

$$\gamma_i \cdot g_t^{(i)}$$

aus $\frac{r_t \cdot h_i}{t_i} = r_t \cdot u_i$ verschiedenen Substitutionen besteht, welche ebenso wie diejenigen von γ_i und von $g_t^{(i)}$ in der Gruppe $g_z^{(i)}$ enthalten sind. Zudem ist der gedachte Komplex eine Gruppe. Ist nämlich s eine Substitution der Gruppe γ_i, also als eine auch in $g_z^{(i)}$ enthaltene Substitution von der Form

$$s_i \cdot \sigma \cdot s_i^{-1},$$

wo σ in g_z, so findet sich

$$s \cdot g_t^{(i)} \cdot s^{-1} = s \cdot s_i g_t s_i^{-1} \cdot s^{-1} = s_i \cdot \sigma g_t \sigma^{-1} \cdot s_i^{-1},$$

also mit Rücksicht auf die an die Formel (36) geknüpfte Bemerkung

$$s \cdot g_t^{(i)} \cdot s^{-1} = s_i g_t s_i^{-1} = g_t^{(i)}.$$

Für jede Substitution s in γ_i und jede Substitution t in $g_t^{(i)}$ kann man daher eine zweite Substitution t_1 in $g_t^{(i)}$ finden, derart, daß $st = t_1 s$ ist. Sind also s, s' zwei Substitutionen in γ_i und t, t' zwei solche in $g_t^{(i)}$, so wird

$$st \cdot s't' = s \cdot ts' \,.\, t' = ss' \cdot t_1 t',$$

d. h. von der Form $s''t''$ sein, wo s'' zu γ_i und t'' zu $g_t^{(i)}$ gehört. Demzufolge ist der Komplex $\gamma_i \cdot g_t^{(i)}$ in der Tat eine Gruppe und ihr Grad $r_t \cdot u_i$ ein Teiler des Grades der Gruppe $g_z^{(i)}$, d. h.

$$(61) \qquad r_z = r_t u_i \cdot v_i.$$

Beachtet man nun in der Formel (59) der Reihe nach die durch die Formeln (50), (60), (61) und (54) gegebenen Beziehungen, so ergibt sich

$$(62) \qquad f_i = v_i$$

als der Grad des Primideals $\mathfrak{p}_i$, den wir suchten.

Endlich sei $N_{\mathfrak{k}}(\mathfrak{P}_{i,k})$ die Relativnorm des Primideals $\mathfrak{P}_{i,k}$ in bezug auf den Körper $\mathfrak{k}$, d. h. das Produkt der

Faktoren $s\mathfrak{P}_{i,k}$, in denen s jede der Substitutionen der Gruppe g bedeutet. Der Formel (49) entsprechend entstehen durch diese Substitutionen nur die Primideale

$$\mathfrak{P}_{i1},\ \mathfrak{P}_{i2},\ \cdots,\ \mathfrak{P}_{i,e_i}$$

jedes von ihnen $h_i = t_i u_i$ Mal, und man findet also mit Rücksicht auf die Formel (55)

$$N_{\mathfrak{k}}(\mathfrak{P}_{i,k}) = \mathfrak{p}_i^{u_i}. \tag{63}$$

Der Wert des Exponenten x_i in der Formel (53):

$$\mathfrak{G}\mathfrak{p}_i = (\mathfrak{P}_{i1}\mathfrak{P}_{i2}\cdots\mathfrak{P}_{i,e_i})^{x_i}$$

läßt sich auch folgendermaßen ermitteln.

Man verstehe unter $\mathfrak{P}$ in Nr. 6 das Primideal $\mathfrak{P}_i = \mathfrak{P}_{i,1}$ und unter $\mathfrak{s}^\varphi$ die niedrigste Potenz der dort mit $\mathfrak{s}$ bezeichneten Substitution, für welche $\varphi > 0$ und

$$\mathfrak{s}^\varphi t = s$$

ist, unter t eine Substitution der Trägheitsgruppe, unter s eine solche der Gruppe g verstanden. Aus (32) folgt allgemein

$$\mathfrak{s}^k \mathrm{P} \equiv \mathrm{P}^{p^k} \pmod{\mathfrak{P}_i}$$

also, da $t\mathrm{P} \equiv \mathrm{P} \pmod{\mathfrak{P}_i}$ ist,

$$s\mathrm{P} = \mathfrak{s}^\varphi t\mathrm{P} \equiv \mathfrak{s}^\varphi \mathrm{P} \equiv \mathrm{P}^{p^\varphi} \pmod{\mathfrak{P}_i}$$

und daher allgemeiner für jede ganze Zahl Ω des Körpers $\mathfrak{K}$ die Kongruenz

$$s\Omega \equiv \Omega^{p^\varphi} \pmod{\mathfrak{P}_i};$$

insbesondere wird also für jede ganze Zahl ω des Körpers $\mathfrak{k}$, da $s\omega = \omega$ ist,

$$\omega \equiv \omega^{p^\varphi} \pmod{\mathfrak{P}_i},$$

d. h.

$$\omega \equiv \omega^{p^\varphi} \pmod{\mathfrak{p}_i}$$

sein; demnach ist φ nicht kleiner als der Grad f_i des Primideals $\mathfrak{p}_i$, d. i. der Exponent von p in der Formel

$$n(\mathfrak{p}_i) = p^{f_i}.$$

Andererseits folgt aus der Formel

$$\omega \equiv \omega^{p^{f_i}} \pmod{\mathfrak{p}_i}$$

des Fermatschen Satzes für jede ganze Zahl ω in $\mathfrak{k}$ auch die Kongruenz

$$\omega \equiv \omega^{p^{f_i}} \pmod{\mathfrak{P}_i}.$$

Nun ist P Wurzel einer Gleichung r^{ten} Grades mit Koeffizienten, welche ganze Zahlen $\omega', \omega'', \cdots$ in $\mathfrak{k}$ sind, sodaß eine Identität stattfindet

$$\mathrm{P}^r + \omega' \mathrm{P}^{r-1} + \omega'' \mathrm{P}^{r-2} + \cdots = 0,$$

und aus dieser ergibt sich durch wiederholte Erhebung zur p^{ten} Potenz eine andere, welche, als Kongruenz (mod. $\mathfrak{P}_i$) aufgefaßt, sich schreiben läßt, wie folgt:

$$\mathrm{P}^{r p^{f_i}} + \omega' \mathrm{P}^{(r-1)p^{f_i}} + \omega'' \mathrm{P}^{(r-2)p^{f_i}} + \cdots \equiv 0 \pmod{\mathfrak{P}_i}.$$

Demnach ist $\mathrm{P}^{p^{f_i}}$ mit einer der Wurzeln derselben Gleichung r^{ten} Grades, d. h. mit einer der zu P relativ Konjugierten, welche durch die Substitutionen der Gruppe g aus P entstehen, (mod. $\mathfrak{P}_i$) kongruent, etwa, wenn s eine solche Substitution bedeutet,

$$\mathrm{P}^{p^{f_i}} \equiv s\mathrm{P} \pmod{\mathfrak{P}_i}$$

oder

$$\mathsf{z}^{f_i}\mathrm{P} \equiv s\mathrm{P} \pmod{\mathfrak{P}_i},$$

allgemeiner ist also für jede ganze Zahl Ω in $\mathfrak{K}$

$$\mathsf{z}^{f_i}\Omega \equiv s\Omega \pmod{\mathfrak{P}_i},$$

eine Kongruenz, welche sich auch schreiben läßt in der Form

$$\mathsf{z}^{-f_i} s\Omega \equiv \Omega \pmod{\mathfrak{P}_i}$$

und eine Gleichung nach sich zieht, wie die folgende:

$$\mathsf{z}^{-f_i}s = t \quad \text{oder} \quad \mathsf{z}^{f_i}t = s;$$

ihr zufolge ist φ nicht größer als f_i, und somit ist

$$\varphi = f_i.$$

Setzt man nun $\mathfrak{p}_i = \mathfrak{P}_i \mathfrak{Q}_i$, so folgt durch Bestimmung der Relativnorm mit Bezug auf $\mathfrak{k}$ die Gleichung

$$\mathfrak{p}_i^r = N_{\mathfrak{k}}(\mathfrak{P}_i) \cdot N_{\mathfrak{k}}(\mathfrak{Q}_i),$$

folglich ist $N_{\mathfrak{k}}(\mathfrak{P}_i)$ eine Potenz von $\mathfrak{p}_i$, etwa

$$N_{\mathfrak{k}}(\mathfrak{P}_i) = \mathfrak{p}_i^{\psi}.$$

Nach der Formel $N(\mathfrak{P}_i) = n N_{\mathfrak{k}}(\mathfrak{P}_i)$ findet sich also die Gleichung

$$p^f = p^{f_i \psi}$$

oder

$$f = f_i \cdot \psi.$$

Hiernach übersieht man mit Beachtung der Gleichung (35) leicht, daß die Gruppe γ_i, welche den Gruppen g und $g_z^{(i)}$ gemeinsam ist, durch die Summe von Komplexen

$$\gamma_i^{(i)} + z^{f_i} \cdot \gamma_i^{(i)} + \cdots + z^{(\psi - 1) f_i} \cdot \gamma_i^{(i)}$$

darstellbar ist, woraus die neue Gleichung $h_i = t_i \cdot \psi$ und aus deren Vergleichung mit (60) die andere:

$$\psi = u_i$$

hervorgeht. Setzt man dies in die obige Formel für die Relativnorm von $\mathfrak{P}_i$ ein und bedenkt, wie bei Herleitung von (63), daß der Primfaktor $\mathfrak{P}_i = \mathfrak{P}_{i1}$ zur Linken jener Formel sich $h_i = t_i u_i$ Mal, zur Rechten aber wegen (53) sich $x_i u_i$ Mal vorfindet, so folgt

$$x_i = t_i$$

und demnach wieder die Formeln (55) und (56).

9. Nach Herleitung dieser allgemeinen Resultate wenden wir uns zur Betrachtung besonderer Unterkörper von $\mathfrak{K}$.

Sei zunächst $\mathfrak{k}$ der Zerlegungskörper $\mathfrak{k}_z$. Dann ist $g = g_z$ und $r = r_z$, mithin wird γ_0, d. i. die Gruppe, welche den Gruppen g_z und $s_0 g_z s_0^{-1} = g_z$ gemeinsam ist, identisch mit g_z, ihr Grad h_0 identisch mit r_z, und daher nach Formel (50) e_0 gleich 1 sein. Zugleich wird der größte gemeinsame Teiler von g_t und g die Gruppe g_t, ihr Grad $t_0 = r_t$, wegen der Formel $h_i = t_i u_i$ und mit Rücksicht auf (40) also $u_0 = f$, mithin $v_0 = 1$ und wegen $r_t = d_0 t_0$ endlich $d_0 = 1$ sein. Infolge hiervon nehmen die allgemeinen Formeln (55) und (56) für den Zerlegungskörper und für $i = 0$ die besondere Gestalt an:

$$\mathfrak{p}_0 = \mathfrak{P}_{01}^{r_t}, \quad p = \mathfrak{p}_0 \cdot \mathfrak{q},$$

wo $\mathfrak{P}_{01}$ mit dem Primidealfaktor $\mathfrak{P}$ von p im Galoisschen Körper gleichbedeutend ist, und $\mathfrak{q}$ ein durch $\mathfrak{p}_0$ nicht teilbares Ideal des Körpers $\mathfrak{k}_z$ bezeichnet; desgleichen findet man aus den Formeln (57), (62), (63) die Gleichungen

$$n(\mathfrak{p}_0) = p, \quad N_{\mathfrak{k}_z}(\mathfrak{P}) = \mathfrak{p}_0^f.$$

Im Zerlegungskörper ist also $\mathfrak{P}^{r_t}$ ein Primidealfaktor von p vom ersten Grade, der mit $\mathfrak{p}_z$ bezeichnet werde und im *Galois*schen Körper in r_t gleiche Primidealfaktoren $\mathfrak{P}$ vom Grade f zerfällt.

Sei zweitens $\mathfrak{k}$ der Trägheitskörper $\mathfrak{k}_t$, folglich $g = g_t$, $r = r_t$ und daher γ_0 als die den Gruppen g und $s_0 g_z s_0^{-1} = g_z$ gemeinsame Gruppe identisch mit g_t, ihr Grad h_0 identisch mit r_t, also $e_0 = 1$. Dann ist ferner der größte gemeinsame Teiler von g und g_t identisch mit der letzteren Gruppe, daher $t_0 = r_t$, $u_0 = 1$, $v_0 = f$; wegen $r_t = d_0 t_0$ ist endlich $d_0 = 1$. Somit gehen die allgemeinen Formeln in diesem Falle über in die folgenden:

$$p = \mathfrak{p}_0 \cdot \mathfrak{q}, \quad \mathfrak{p}_0 = \mathfrak{P}^{r_t},$$
$$n(p_0) = p^f, \quad N_{\mathfrak{k}_t}(\mathfrak{P}) = \mathfrak{p}_0,$$

welche lehren, daß beim Übergange vom Zerlegungskörper zum Trägheitskörper, der ihn in sich enthält, das Primideal $\mathfrak{p}_z$, das im Körper $\mathfrak{k}_t$ mit $\mathfrak{p}_t$ bezeichnet werde, keine Zerlegung, sondern nur eine Graderhöhung erfährt, indem das Primideal, das im Zerlegungskörper vom ersten Grade ist, im Trägheitskörper vom Grade f wird. Des letztern Umstandes wegen zerfallen die ganzen Zahlen des Trägheitskörpers (mod. $\mathfrak{P}^{r_t}$) in p^f Klassen kongruenter Zahlen. Nun gehören zwei Zahlen einer Klasse (mod. $\mathfrak{P}^{r_t}$) auch zu derselben Klasse (mod. $\mathfrak{P}$); sind umgekehrt zwei ganze Zahlen des Trägheitskörpers einander (mod. $\mathfrak{P}$) kongruent, so gehört ihre Differenz sowohl zum Trägheitskörper als auch zum Ideale $\mathfrak{P}$ und daher zur Gesamtheit $\mathfrak{p}_t = \mathfrak{P}^{r_t}$ der ihnen beiden gemeinsamen Zahlen, jene zwei Zahlen sind also einander auch (mod. $\mathfrak{P}^{r_t}$) kongruent. Daher ist die Verteilung der ganzen Zahlen des Trägheitskörpers in Klassen (mod. $\mathfrak{P}^{r_t}$) die gleiche wie (mod. $\mathfrak{P}$), also p^f auch die Anzahl ihrer Klassen (mod. $\mathfrak{P}$). Die Zahlen des Trägheitskörpers gehören aber sämtlich zum Körper $\mathfrak{K}$, dessen ganze Zahlen wegen (28) auch genau in p^f Klassen (mod. $\mathfrak{P}$) zerfallen; demnach muß jede Zahl des *Galois*schen Körpers einer Zahl des Trägheitskörpers (mod. $\mathfrak{P}$) kongruent sein.

Der Trägheitskörper $\mathfrak{k}_t$ vom Grade $n_t = \frac{N}{r_t}$ ist in bezug auf den Zerlegungskörper $\mathfrak{k}_z$ vom Grade $n_z = \frac{N}{r_z}$ ein Relativkörper vom Grade $\frac{N}{r_t} : \frac{N}{r_z} = \frac{r_z}{r_t} = f$. Ist daher θ eine ihn erzeugende ganze Zahl, so leistet diese einer in $\mathfrak{k}_z$ irreduktibeln Gleichung f^{ten} Grades

$$\theta^f + c_1\theta^{f-1} + c_2\theta^{f-2} + \cdots + c_f = 0 \tag{64}$$

Genüge, deren Koeffizienten ganze Zahlen in $\mathfrak{k}_z$ sind. Die zu θ relativ konjugierten anderen Wurzeln dieser Gleichung werden gefunden, wenn man diejenigen Substitutionen der Zerlegungsgruppe verwendet, welche der Trägheitsgruppe nicht angehören, nämlich die Substitutionen

$$s_0 = 1,\ z,\ z^2,\ \cdots,\ z^{f-1}. \tag{65}$$

Ist aber θ eine Zahl in $\mathfrak{k}_t$, so gehört auch $z\theta$ dem Körper $\mathfrak{k}_t$ an. Denn zu jeder Substitution t der Trägheitsgruppe gibt es eine Substitution t' dieser selben Gruppe so beschaffen, daß $tz = zt'$ ist; da nun für jede Zahl θ in $\mathfrak{k}_t$ die Gleichung $t'\theta = \theta$ besteht, so folgt hieraus für jede Substitution t der Trägheitsgruppe die andere Gleichung

$$tz\theta = zt'\theta = z\theta$$

und folglich ist $z\theta$ eine Zahl des Trägheitskörpers. Wenn also θ, wie zuvor angenommen, eine erzeugende Zahl des letzteren ist, so ist $z\theta$ rational durch θ ausdrückbar. Demnach ist die Gleichung f^{ten} Grades (64) eine im Rationalitätsbereiche $\mathfrak{k}_z$ *Galois*sche Gleichung mit der zyklischen Substitutionsgruppe (65) vom Grade f.

10. Der Trägheitskörper seinerseits ist nun in einer Reihe anderer Unterkörper von $\mathfrak{K}$ enthalten, von denen jeder den ihm vorangehenden umfaßt und denen die besondere Bedeutung zukommt, daß beim Übergange vom einen zum andern das Primideal $\mathfrak{p}_0 = \mathfrak{P}^{r_t}$ gradweise sich immer weiter zerlegt, bis man, zum Körper $\mathfrak{K}$ gelangend, auf das Primideal $\mathfrak{P}$ selbst stößt. Das Verdienst, dies nachgewiesen zu haben, gebührt Hilbert.

Dem 6. Kapitel, Nr. 22 ist eine ganze Zahl P oder $P(\varrho)$ des Körpers $\mathfrak{K}$ zugrunde gelegt, welche die Eigenschaft hat, daß P zwar durch das Primideal $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist. Unter allen (mod. $\mathfrak{P}$) kongruenten Zahlen dieser Art gibt es (vgl. Kap. 7, Ende von Nr. 15) auch eine den Körper $\mathfrak{K}$ **erzeugende** ganze Zahl; als solche sei P hier gewählt. Da nun, wenn wieder P die Primitivzahl (mod. $\mathfrak{P}$) bezeichnet, die wir in Nr. 6 eingeführt haben, alle ganzen Zahlen in $\mathfrak{K}$ einer der folgenden:

$$0,\ 1,\ \mathrm{P},\ \mathrm{P}^2,\ \cdots,\ \mathrm{P}^{p^f-2}$$

(mod. $\mathfrak{P}$) kongruent sind, so werden die Zahlen

$$0,\ P,\ \mathrm{P}P,\ \mathrm{P}^2 P,\ \cdots,\ \mathrm{P}^{p^f-2} P$$

p^f in $\mathfrak{P}$ enthaltene aber (mod. $\mathfrak{P}^2$) inkongruente Zahlen sein, und da

$$(\mathfrak{G},\ \mathfrak{P}^2) = (\mathfrak{G},\ \mathfrak{P}) \cdot (\mathfrak{P},\ \mathfrak{P}^2)$$

d. i. $p^{2f} = p^f \cdot (\mathfrak{P}, \mathfrak{P}^2)$, mithin $(\mathfrak{P}, \mathfrak{P}^2) = p^f$ ist, ein vollständiges Restsystem des Modulus $\mathfrak{P}$ in bezug auf $\mathfrak{P}^2$ darstellen, jede Zahl in $\mathfrak{P}$ wird also einer von ihnen (mod. $\mathfrak{P}^2$) kongruent sein. Ist aber t_i irgend eine Substitution der Trägheitsgruppe, also für jede ganze Zahl Ω in $\mathfrak{K}$

$$t_i\Omega \equiv \Omega \text{ (mod. } \mathfrak{P}),$$

insbesondere $t_i P \equiv P \equiv 0$ (mod. $\mathfrak{P}$), aber nicht $t_i P \equiv 0$ (mod. $\mathfrak{P}^2$), so ergibt sich für jede Substitution t_i der Trägheitsgruppe eine Kongruenz von der Form

$$t_i P \equiv \mathrm{P}^{a_i} \cdot P \text{ (mod. } \mathfrak{P}^2), \tag{66}$$

in welcher a_i eine der Zahlen $0, 1, 2, \cdots, p^{f-2}$ bezeichnet. Unter diesen Exponenten a_i sei a der kleinste positive, sodaß für eine gewisse Substitution t der Trägheitsgruppe die Kongruenz besteht

$$tP \equiv \mathrm{P}^a \cdot P \text{ (mod. } \mathfrak{P}^2), \tag{67}$$

welche, wenn allgemein $(\mathfrak{P}^m)$ eine in $\mathfrak{P}^m$ enthaltene Zahl bedeutet, mit der Gleichung

$$tP = \mathrm{P}^a \cdot P + (\mathfrak{P}^2)$$

gleichbedeutend ist. Hieraus folgt

$$t^2 P = (t\mathrm{P})^a \cdot tP + (\mathfrak{P}^2)$$

d. i.

$$t^2 P = (\mathrm{P}^a + (\mathfrak{P})) \cdot (\mathrm{P}^a P + (\mathfrak{P}^2)) + (\mathfrak{P}^2)$$

oder die Kongruenz

$$t^2 P \equiv \mathrm{P}^{2a} \cdot P \pmod{\mathfrak{P}^2}$$

und allgemeiner

$$(68) \qquad t^m P \equiv \mathrm{P}^{ma} \cdot P \pmod{\mathfrak{P}^2}.$$

Wenn daher k die kleinste positive Zahl ist von der Beschaffenheit, daß t^k die identische Substitution s_0 und folglich $t^k P = P$ wird, so findet sich $\mathrm{P}^{ka} \equiv 1 \pmod{\mathfrak{P}}$ also

$$(69) \qquad t^{-m} P = t^{k-m} P \equiv \mathrm{P}^{-ma} \cdot P \pmod{\mathfrak{P}^2}.$$

In Verbindung mit (66) ergibt sich hieraus die Kongruenz

$$t^{-m} t_i P \equiv \mathrm{P}^{a_i - ma} \cdot P \pmod{\mathfrak{P}^2},$$

während $t^{-m} t_i$ auch eine Substitution der Trägheitsgruppe ist. Daher muß a_i ein Vielfaches von a sein, denn sonst wäre $a_i - ma$ für eine passend gewählte ganze Zahl m positiv und kleiner als a, gegen die Bedeutung dieses Zeichens. Da nun nach (68) jedes Vielfache von a zu den Zahlen a_i gehört oder einer von ihnen nach dem Modulus $p^f - 1$ kongruent ist, so werden, wenn h die Anzahl der verschiedenen a_i bedeutet, die Vielfachen

$$(70) \qquad 0,\ a,\ 2a,\ \cdots,\ (h-1)a$$

diese sämtlich darstellen und ha gleich $p^f - 1$ sein müssen. Die Zahl h ist hiernach ein Teiler von $p^f - 1$ und daher relativ prim gegen p.

Dies vorausgeschickt, nenne man jetzt v_i jede Substitution der Trägheitsgruppe, für welche der ihr nach (66) entsprechende Exponent a_i gleich Null, also

$$(71) \qquad v_i P \equiv P \pmod{\mathfrak{P}^2}$$

ist. Offenbar hat die Gesamtheit dieser Substitutionen v_i wieder den Charakter einer Gruppe und bildet also eine Untergruppe der Trägheitsgruppe, welche von Hilbert die Verzweigungsgruppe g_v des Primideals $\mathfrak{P}$ genannt worden ist; ihr Grad, der ein Teiler des Grades r_t der Trägheitsgruppe

sein muß, heiße r_v, der zur Verzweigungsgruppe zugeordnete Unterkörper von $\mathfrak{K}$ heiße $\mathfrak{k}_v$ und der Verzweigungskörper des Primideals $\mathfrak{P}$, und n_v sei sein Grad. Wäre die Kongruenz (71) für alle Substitutionen der Trägheitsgruppe erfüllt d. h., wäre $h = 1$, so fiele die Verzweigungsgruppe g_v mit der Trägheitsgruppe g_t und folglich $\mathfrak{k}_v$ mit $\mathfrak{k}_t$ zusammen. Aus (71) folgt

$$v_t P - P = \mathfrak{P}^2 \cdot \mathfrak{Q}, \tag{72}$$

wo $\mathfrak{Q}$ ein Ideal des Körpers $\mathfrak{K}$ bedeutet. Da $P^2 = \mathfrak{P}^2 \cdot \mathfrak{A}$ und das Ideal $\mathfrak{A}$ durch $\mathfrak{P}$ nicht teilbar ist, so folgt

$$\mathfrak{A} \cdot (v_t P - P) = P^2 \cdot \mathfrak{Q}$$

d. h. für jede Zahl α in $\mathfrak{A}$ gibt es eine Zahl q in $\mathfrak{Q}$ der Art, daß

$$\alpha \cdot (v_t P - P) = P^2 \cdot q$$

ist, mithin findet sich, wenn α nicht teilbar durch $\mathfrak{P}$ und $\alpha\gamma \equiv 1 \pmod{\mathfrak{P}}$ gewählt wird, für $Q = q\gamma$ die Kongruenz

$$v_t P \equiv P + P^2 Q \pmod{\mathfrak{P}^3}$$

oder die Gleichung

$$v_t P = P + P^2 Q + (\mathfrak{P}^3),$$

aus welcher wieder die andere:

$$v_t^2 P = v_t P + v_t P^2 \cdot v_t Q + (\mathfrak{P}^3)$$

hervorgeht, während

$$v_t P^2 = (v_t P)^2 = P^2 + (\mathfrak{P}^3),\ v_t Q = Q + (\mathfrak{P})$$

ist, letzteres, da v_t zur Trägheitsgruppe gehört. Hieraus folgt aber

$$v_t^2 P \equiv P + 2 P^2 Q \pmod{\mathfrak{P}^3},$$

ebenso

$$v_t^3 P \equiv P + 3 P^2 Q \pmod{\mathfrak{P}^3}$$

usw., endlich also

$$v_t^p P \equiv P \pmod{\mathfrak{P}^3}.$$

In gleicher Weise gelangt man zu den weiteren Formeln

$$v_t^{p^2} P \equiv P \pmod{\mathfrak{P}^4}$$

usw., allgemein

(73) $$v_i^{p^{m-2}} P \equiv P \pmod{\mathfrak{P}^m}.$$

Hier bezeichnet $v_i^{p^{m-2}}$ eine gewisse Substitution der Verzweigungsgruppe. Bestimmt man aber für alle von s_0 verschiedenen Substitutionen v dieser Gruppe die höchste in $vP - P$ aufgehende Potenz von $\mathfrak{P}$ und nennt $\mathfrak{P}^u$ die höchste sämtlicher so erhaltenen Potenzen[1]), derart, daß für keine jener Substitutionen v die Kongruenz

$$vP \equiv P \pmod{\mathfrak{P}^{u+1}}$$

bestehen kann, so folgt aus (73) für $m = u + 1$, daß

$$v_i^{p^{u-1}} = s_0$$

nämlich gleich der identischen Substitution sein muß. Daher ist der kleinste Exponent k, für welchen $v_i^k = s_0$ wird, ein Teiler von p^{u-1}, d. i. eine Potenz von p, und Gleiches gilt deshalb auch vom Grade der Gruppe: r_v muß eine Potenz von p, etwa

$$r_v = p^l$$

sein. Da nun die für jede Substitution t_i der Trägheitsgruppe bestehende Kongruenz (66) dem Voraufgeschickten zufolge in der Gestalt

$$t_i P \equiv \mathrm{P}^{ma} \cdot P \pmod{\mathfrak{P}^2}$$

geschrieben werden kann, wo m eine der Zahlen $0, 1, 2, \cdots h-1$, so folgt, unter t die oben so bezeichnete Substitution derselben Gruppe verstanden, die andere Kongruenz

$$t^{-m} t_i P \equiv P \pmod{\mathfrak{P}^2},$$

derzufolge die Substitution $t^{-m} t_i$ zur Verzweigungsgruppe gehört; setzt man demnach $t^{-m} t_i = v$, so findet sich jede Substitution der Trägheitsgruppe von der Gestalt

(74) $$t_i = t^m \cdot v,$$

und, da auch alle Substitutionen von dieser Gestalt zur Trägheitsgruppe gehören und offenbar voneinander verschieden sind, die im *Galois*schen Sinne zu nehmende Gleichung

1) Eine solche gibt es, da P als Erzeugende des Körpers $\mathfrak{K}$ gewählt worden ist, mithin $vP - P$ für alle bezeichneten Substitutionen v von Null verschieden ist.

(75) $$g_t = g_v + t \cdot g_v + t^2 \cdot g_v + \cdots + t^{h-1} \cdot g_v,$$

welche aussagt, daß die Gruppe g_t aus den h Komplexen

(76) $$g_v,\ t \cdot g_v,\ t^2 \cdot g_v,\ \cdots,\ t^{h-1} \cdot g_v$$

zusammengesetzt ist. Hiernach ist

(77) $$r_t = h \cdot r_v = h \cdot p^l.$$

Ferner aber folgt für den Wert von m, welcher in (74) gedacht wird, aus der Kongruenz (69) leicht die nachstehende:

$$t_i t^{-m} P \equiv P \pmod{\mathfrak{P}^2},$$

aus welcher $t_i t^{-m}$ sich als eine Substitution v' der Verzweigungsgruppe d. i.

$$t_i = v' t^m$$

sich erweist; durch Vergleichung mit (74) folgt

$$v' t^m = t^m v$$

also

(78) $$v' = t^m v t^{-m}$$

oder die „Invarianz" der Verzweigungsgruppe.

Endlich kann die Verzweigungsgruppe als die Gesamtheit derjenigen Substitutionen v_i der Gruppe G definiert werden, bei deren Anwendung die Kongruenz

(79) $$v_i \Omega \equiv \Omega \pmod{\mathfrak{P}^2}$$

für jede ganze Zahl Ω des Körpers $\mathfrak{K}$ erfüllt ist. In der Tat ist Ω nach voriger Nummer einer Zahl ω des Trägheitskörpers (mod. $\mathfrak{P}$) kongruent:

$$\Omega - \omega \equiv 0 \pmod{\mathfrak{P}}.$$

Dem Obigen zufolge besteht daher eine der beiden Kongruenzen

$$\Omega - \omega \equiv 0 \quad \text{oder} \quad \Omega - \omega \equiv \mathrm{P}^\alpha \cdot P \pmod{\mathfrak{P}^2},$$

wo α eine Zahl aus der Reihe $0, 1, 2, \cdots, p^f - 2$. Wenn nun erstens v_i eine Substitution der Verzweigungsgruppe ist, also auch zur Trägheitsgruppe gehört und demnach ω ungeändert läßt, so findet sich im zweiten Falle durch deren Anwendung

$$v_i \mathfrak{Q} - \omega \equiv v_i \mathrm{P}^\alpha \cdot v_i P \pmod{\mathfrak{P}^2},$$

wo nun

$$v_i \mathrm{P}^\alpha = \mathrm{P}^\alpha + (\mathfrak{P}), \quad v_i P = P + (\mathfrak{P}^2)$$

ist, ersteres, da v_i zur Trägheitsgruppe gehört, letzteres wegen (71). Also wird

$$v_i \mathfrak{Q} - \omega = \mathrm{P}^\alpha P + (\mathfrak{P}^2)$$

d. h. $v_i \mathfrak{Q} - \omega \equiv \mathrm{P}^\alpha P \equiv \mathfrak{Q} - \omega \pmod{\mathfrak{P}^2}$, eine Kongruenz, die sich auch im ersteren Falle ergibt. Daher ist für jede ganze Zahl $\mathfrak{Q}$ in $\mathfrak{K}$

$$v_i \mathfrak{Q} \equiv \mathfrak{Q} \pmod{\mathfrak{P}^2}.$$

Ist aber zweitens diese Kongruenz für jede ganze Zahl $\mathfrak{Q}$ in $\mathfrak{K}$ erfüllt, so findet sie auch für $\mathfrak{Q} = P$ statt, d. h. v_i erfüllt die Kongruenz (71), und da zugleich auch die Kongruenz

$$v_i \mathfrak{Q} \equiv \mathfrak{Q} \pmod{\mathfrak{P}}$$

für jede Zahl $\mathfrak{Q}$ in $\mathfrak{K}$ besteht, so gehört v_i der Trägheitsgruppe an und muß speziell eine Substitution der Verzweigungsgruppe sein.

Wird jetzt unter dem in Nr. 7 mit $\mathfrak{k}$ bezeichneten Körper der Verzweigungskörper verstanden, also

$$\mathfrak{k} = \mathfrak{k}_v, \; g = g_v, \; r = r_v = p^l$$

gesetzt, so wird γ_0 die Gesamtheit der in g_v und g_z enthaltenen Substitutionen, d. i. $\gamma_0 = g_v$, mithin $h_0 = r_v$ und $e_0 = 1$. Ferner wird die Gesamtheit der den Gruppen g und g_t gemeinsamen Substitutionen identisch mit g_v, demnach $t_0 = r_v$, $u_0 = 1$, $v_0 = f$. Endlich folgt wegen (77) aus der Gleichung $r_t = d_0 t_0$ noch $d_0 = h$. Somit nehmen die allgemeinen Formeln der Nr. 8 hier die Gestalt an

$$\mathfrak{S}\mathfrak{p}_0 = \mathfrak{P}^{r_v}, \; n(\mathfrak{p}_0) = p^f$$

und lehren, daß $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ ein Primidealfaktor von p im Verzweigungskörper und f sein Grad ist, daß mithin das Primideal $\mathfrak{p}_z = \mathfrak{p}_t = \mathfrak{P}^{r_t}$ beim Übergange zum Verzweigungskörper, welcher den Trägheitskörper in sich enthält, sich nach der Beziehung

$$\mathfrak{p}_z = \mathfrak{p}_t = \mathfrak{p}_v^{\,h}$$

in h gleiche Primidealfaktoren $\mathfrak{p}_v$ vom f^{ten} Grade zerlegt.

Der Verzweigungskörper $\mathfrak{k}_v$ vom Grade $n_v = \frac{N}{r_v}$ ist in bezug auf den Trägheitskörper $\mathfrak{k}_t$ vom Grade $n_t = \frac{N}{r_t}$ ein Relativkörper vom Grade $\frac{n_v}{n_t} = \frac{r_t}{r_v} = h$. Eine ihn erzeugende ganze Zahl η leistet daher einer in $\mathfrak{k}_t$ irreduktibeln Gleichung h^{ten} Grades

$$\eta^h + d_1\eta^{h-1} + d_2\eta^{h-2} + \cdots + d_h = 0 \tag{80}$$

Genüge, deren Koeffizienten ganze Zahlen in $\mathfrak{k}_t$ sind; die zu η relativ Konjugierten, d. i. die übrigen Wurzeln dieser Gleichung entstehen durch diejenigen Substitutionen der Trägheitsgruppe, welche der Verzweigungsgruppe nicht angehören, nämlich durch die h Wiederholungen

$$t^0 = s_0,\ t^1,\ t^2,\ \cdots,\ t^{h-1} \tag{81}$$

der im Obigen mit t bezeichneten Substitution der Trägheitsgruppe. Ist aber η eine Zahl in $\mathfrak{k}_v$, so ist's auch die Zahl $t^m\eta$, wo t^m irgend eine der Substitutionen (81) bezeichnet. Denn zu jeder Substitution v' der Verzweigungsgruppe gehört nach (78) eine andere Substitution v derselben, für welche $t^m v = v' t^m$ ist. Da nun für jede Zahl η in $\mathfrak{k}_v$ die Gleichung $v\eta = \eta$ erfüllt ist, so folgt hieraus für jede Substitution v' der Verzweigungsgruppe

$$v' t^m \eta = t^m v \eta = t^m \eta,$$

folglich gehört die Zahl $t^m\eta$ dem Verzweigungskörper an. Ist demnach η eine erzeugende Zahl des letztern, so muß $t^m\eta$ eine rationale Funktion von η sein und demnach ist die Gleichung (80) eine relativ zu $\mathfrak{k}_t$ *Galois*sche Gleichung mit der zyklischen Gruppe der Substitutionen (81) vom Grade h.

11. Da für jede Substitution v_i der Verzweigungsgruppe die Kongruenz (71) besteht, so ist es möglich, daß dieselbe auch noch für eine höhere als die zweite Potenz von $\mathfrak{P}$ als Modulus stattfindet. Man bezeichne also mit $\mathfrak{P}^\lambda$ die höchste Potenz von $\mathfrak{P}$, in bezug auf welche die Kongruenz

$$v_i P \equiv P \pmod{\mathfrak{P}^\lambda} \tag{82}$$

für jede Substitution v_i der Zerlegungsgruppe erfüllt ist, sodaß nicht jede solche Substitution auch noch die Kongruenz

$$v_i P \equiv P \pmod{\mathfrak{P}^{\lambda+1}}$$

erfüllt. Dann bilden wieder diejenigen Substitutionen $\bar{v}_i$ der Verzweigungsgruppe, für welche noch

$$(83) \qquad \bar{v}_i P \equiv P \pmod{\mathfrak{P}^{\lambda+1}}$$

ist, eine neue Untergruppe derselben, welche die **einmal überstrichene Verzweigungsgruppe** $g_{\bar{v}}$ des Primideals $\mathfrak{P}$ genannt werde; der zugeordnete Körper $\mathfrak{k}_{\bar{v}}$ heiße entsprechend der **einmal überstrichene Verzweigungskörper des Primideals** $\mathfrak{P}$; sein Grad sei $n_{\bar{v}}$, $r_{\bar{v}}$ derjenige der Gruppe $g_{\bar{v}}$. Da der letztere ein Teiler von $r_v = p^l$ sein muß, so ist er selbst eine Potenz von p, $r_{\bar{v}} = p^{\bar{l}}$; wir setzen $l - \bar{l} = \bar{e}$, sodaß

$$(84) \qquad r_v = r_{\bar{v}} \cdot p^{\bar{e}}$$

ist. Demnach ist die Gruppe g_v aus $p^{\bar{e}}$ Komplexen von der Form

$$(85) \qquad v_0 \cdot g_{\bar{v}} = g_{\bar{v}}, \quad v_1 \cdot g_{\bar{v}}, \cdots, v_{p^{\bar{e}}-1} \cdot g_{\bar{v}}$$

zusammengesetzt, und es soll gezeigt werden, **daß die $p^{\bar{e}}$, der Gruppe $g_{\bar{v}}$ (mit Ausnahme der ersten) nicht angehörigen Substitutionen**

$$(86) \qquad v_0 = s_0, \quad v_1, v_2, \cdots, v_{p^{\bar{e}}-1}$$

die Eigenschaft haben, daß für zwei beliebige v_i, v_k derselben eine Gleichung

$$(87) \qquad v_i v_k = v_k v_i \cdot \bar{v}$$

besteht, worin $\bar{v}$ eine Substitution der Gruppe $g_{\bar{v}}$ bedeutet. Nach Kap. 6, Nr. 22 kann nämlich (mod. $\mathfrak{P}^{\lambda+1}$) jede ganze Zahl Ω in $\mathfrak{K}$ einem Ausdrucke von der Form

$$\alpha_0 + \alpha_1 P + \alpha_2 P^2 + \cdots + \alpha_\lambda P^\lambda$$

kongruent gesetzt werden, in welchem die Koeffizienten α_i ganze Zahlen in $\mathfrak{K}$ sind. Man darf aber diese Koeffizienten spezieller als ganze Zahlen des Trägheitskörpers voraussetzen. In der Tat ist Ω nach Nr. 9 einer Zahl α_0 des letztern (mod. $\mathfrak{P}$) kongruent, also $\Omega = \alpha_0 + \mathfrak{P} \cdot \mathfrak{Q}$, wo $\mathfrak{Q}$ ein Ideal des Körpers $\mathfrak{K}$; hieraus folgt, wie bei Formel (72)

$$\mathfrak{Q} = \alpha_0 + \alpha_1 P + (\mathfrak{P}^2),$$

während α_1 eine Zahl des Trägheitskörpers bezeichnet, woraus dann, wieder wie bei Formel (72), sich

$$\mathfrak{Q} = \alpha_0 + \alpha_1 P + \alpha_2 P^2 + (\mathfrak{P}^3)$$

ergibt, unter α_2 eine Zahl des Trägheitskörpers verstanden usw., bis die Kongruenz

$$\mathfrak{Q} \equiv \alpha_0 + \alpha_1 P + \alpha_2 P^2 + \cdots + \alpha_\lambda P^\lambda \pmod{\mathfrak{P}^{\lambda+1}}$$

mit in $\mathfrak{k}_t$ liegenden Koeffizienten α_i hervorgeht. Sind nun v_i, v_k zwei beliebige Substitutionen der Verzweigungsgruppe, so erhält man zwei Kongruenzen von der Form

$$(88) \quad v_i P \equiv P + Q_i P^\lambda, \quad v_k P \equiv P + Q_k \cdot P^\lambda \pmod{\mathfrak{P}^{\lambda+1}},$$

in denen Q_i, Q_k ganze Zahlen in $\mathfrak{K}$ bezeichnen. Hiernach findet sich

$$v_k P^\lambda = P^\lambda + (\mathfrak{P}^{\lambda+1}),$$

während $v_k Q_i = Q_i + (\mathfrak{P})$ ist, also erhält man

$$v_k (Q_i P^\lambda) = Q_i P^\lambda + (\mathfrak{P}^{\lambda+1})$$

und demnach aus der ersten der Kongruenzen (88), wenn man auf sie die Substitution v_k anwendet und die zweite jener Kongruenzen berücksichtigt, folgende Kongruenz:

$$v_k v_i P \equiv P + Q_k \cdot P^\lambda + Q_i \cdot P^\lambda \pmod{\mathfrak{P}^{\lambda+1}}.$$

Aus der Symmetrie des Ausdrucks zur Rechten in bezug auf i, k erschließt man aber die Beziehung

$$v_k v_i P \equiv v_i v_k P \pmod{\mathfrak{P}^{\lambda+1}}$$

und nun aus der für $\mathfrak{Q}$ zuvor abgeleiteten Kongruenz, da die α_i bei den in g_t enthaltenen Substitutionen v_i, v_k ungeändert bleiben, allgemein für jede ganze Zahl $\mathfrak{Q}$ in $\mathfrak{K}$ die Kongruenz

oder
$$\left.\begin{aligned} v_k v_i \mathfrak{Q} &\equiv v_i v_k \mathfrak{Q} \\ v_k^{-1} v_i^{-1} v_k v_i \mathfrak{Q} &\equiv \mathfrak{Q} \end{aligned}\right\} \pmod{\mathfrak{P}^{\lambda+1}}.$$

Nun ist aber $v_k^{-1} v_i^{-1} v_k v_i$ eine Substitution der Verzweigungsgruppe; da sie die vorstehende Kongruenz für jede ganze Zahl $\mathfrak{Q}$ in $\mathfrak{K}$ erfüllt, gehört sie sogar der einmal überstrichenen Verzweigungsgruppe $g_{\bar{v}}$ an, und indem man sie als solche mit $\bar{v}$ bezeichnet, gewinnt man die Gleichung

$$v_k^{-1} v_i^{-1} v_k v_i = \bar{v},$$

d. i. für je zwei beliebige Substitutionen v_i, v_k der Gruppe g_v, insbesondere also auch der Reihe (86) die behauptete Beziehung (87). Wird insbesondere v_k als eine Substitution $\bar{v}'$ der Gruppe $g_{\bar{v}}$ vorausgesetzt, so nimmt diese Beziehung die Form an:

$$(89) \qquad \bar{v}' \cdot v_i = v_i \cdot \bar{v}'',$$

worin auch $\bar{v}'' = \bar{v}' \cdot \bar{v}$ eine Substitution in $g_{\bar{v}}$ bedeutet.

Wir wählen jetzt den einmal überstrichenen Verzweigungskörper $\mathfrak{k}_{\bar{v}}$ an Stelle des Unterkörpers $\mathfrak{k}$ der Nr. 7. Aus $\mathfrak{k} = \mathfrak{k}_{\bar{v}}$ ergibt sich dann $g = g_{\bar{v}}$, $r = r_{\bar{v}} = p^{\bar{l}}$, γ_0 wird als die den Gruppen g und g_t gemeinsame Gruppe identisch mit $g_{\bar{v}}$, also $h_0 = r_{\bar{v}}$, $e_0 = 1$; die den Gruppen g und g_t gemeinsame Gruppe wird wieder $g_{\bar{v}}$, mithin $t_0 = r_{\bar{v}}$, $u_0 = 1$, $v_0 = f$; aus

$$r_t = d_0 t_0 = d_0 r_{\bar{v}}$$

und wegen $r_t = h \cdot r_v$ sowie $r_v = p^l$ folgt endlich noch

$$d_0 = h \cdot p^{l-\bar{l}} = h \cdot p^{\bar{e}}.$$

Mit Rücksicht auf diese Werte liefern die allgemeinen Formeln in Nr. 8 für das dort mit $\mathfrak{p}_0$ bezeichnete Primideal des Körpers $\mathfrak{k}_{\bar{v}}$, welches hier $\mathfrak{p}_{\bar{v}}$ heiße, den Wert

$$\mathfrak{p}_{\bar{v}} = \mathfrak{P}^{r_{\bar{v}}} = \mathfrak{P}^{p^{\bar{l}}},$$

während

$$n(\mathfrak{p}_{\bar{v}}) = p^f$$

wird. Somit zerlegt sich das Primideal $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ des f^{ten} Grades des Verzweigungskörpers beim Übergange zu dem ihn umfassenden einmal überstrichenen Verzweigungskörper nach der Formel

$$\mathfrak{p}_v = (\mathfrak{p}_{\bar{v}})^{p^{\bar{e}}}$$

in $p^{\bar{e}}$ gleiche Primidealfaktoren vom Grade f.

Der Körper $\mathfrak{k}_{\bar{v}}$ ist relativ zu $\mathfrak{k}_v$ ein Körper vom Grade $\frac{n_{\bar{v}}}{n_v} = \frac{r_v}{r_{\bar{v}}} = p^{\bar{e}}$. Ist also $\bar{\eta}$ eine ihn erzeugende ganze Zahl, so leistet diese einer in $\mathfrak{k}_v$ irreduktibeln Gleichung vom Grade $p^{\bar{e}}$ und von der Form

$$(90) \qquad \bar{\eta}^{p^{\bar{e}}} + \bar{d}_1 \cdot \bar{\eta}^{p^{\bar{e}}-1} + \cdots + \bar{d}_{p^{\bar{e}}} = 0$$

Genüge, deren Koeffizienten ganze Zahlen in $\mathfrak{k}_v$ sind. Diese Gleichung ist eine relativ zu $\mathfrak{k}_v$ *Abel*sche Gleichung. Denn die zu $\bar{\eta}$ relativ Konjugierten, d. i. die übrigen Wurzeln der vorigen Gleichung entstehen, wenn auf $\bar{\eta}$ diejenigen Substitutionen der Gruppe g_v angewandt werden, welche nicht zur Gruppe $g_{\bar{v}}$ gehören, nämlich die Substitutionen der Reihe (86). Ist nun v_i irgend eine von diesen, so läßt sich zu jeder Substitution $\bar{v}'$ der Gruppe $g_{\bar{v}}$ nach der Formel (89) eine andere Substitution $\bar{v}''$ dieser Gruppe bestimmen, sodaß

$$\bar{v}' \cdot v_i \bar{\eta} = v_i \cdot \bar{v}'' \bar{\eta} = v_i \bar{\eta}$$

gefunden wird, die Zahl $v_i \bar{\eta}$ bleibt also ungeändert bei jeder Substitution in $g_{\bar{v}}$ und gehört mithin dem Körper $\mathfrak{k}_{\bar{v}}$ an, d. h. jede Wurzel der Gleichung (90) ist rational durch $\bar{\eta}$ und die Zahlen des Körpers $\mathfrak{k}_v$ ausdrückbar. Setzt man demgemäß

$$v_i \bar{\eta} = f_i(\bar{\eta}),$$

ebenso, wenn v_k eine andere der Substitutionen (86) bedeutet,

$$v_k \bar{\eta} = f_k(\bar{\eta}),$$

so findet man die Gleichungen

$$v_k v_i \bar{\eta} = f_i(f_k(\bar{\eta})), \quad v_i v_k \bar{\eta} = f_k(f_i(\bar{\eta})),$$

deren erstere auch, wenn unter $\bar{v}$ die in (87) gedachte Substitution verstanden wird, in der folgenden Form:

$$v_k v_i \bar{v} \bar{\eta} = f_i(f_k(\bar{\eta}))$$

geschrieben werden kann und dann wegen (87) die Gleichung

$$f_i(f_k(\bar{\eta})) = f_k(f_i(\bar{\eta}))$$

herbeiführt, welche die bezüglich der Gleichung (90) ausgesprochene Behauptung bestätigt.

12. Man kann nun in gleicher Weise fortfahren. Bedeutet nämlich $\bar{\lambda}$ den höchsten Exponenten der Art, daß bei allen Substitutionen $\bar{v}$ der Gruppe $g_{\bar{v}}$ die Kongruenz

$$\bar{v} P \equiv P$$

zwar (mod. $\mathfrak{P}^{\bar{\lambda}}$) aber nicht mehr (mod. $\mathfrak{P}^{\bar{\lambda}+1}$) erfüllt ist, so bilden diejenigen Substitutionen $\bar{v}$, für welche sie im Gegenteil nach diesem letztern Modulus stattfindet, wieder eine neue in

$g_{\bar{v}}$ enthaltene Gruppe, die zweimal überstrichene Verzweigungsgruppe $g_{\bar{\bar{v}}}$ des Primideals $\mathfrak{P}$, welcher dann der zweimal überstrichene Verzweigungskörper $\mathfrak{k}_{\bar{\bar{v}}}$ desselben zugeordnet ist. Offenbar steht diese neue Gruppe $g_{\bar{\bar{v}}}$ zur Gruppe $g_{\bar{v}}$ in genau der analogen Beziehung, wie die letztere zur Gruppe g_v, und somit gelten auch die analogen Resultate:

Der Grad von $g_{\bar{\bar{v}}}$ ist eine Potenz $p^{\bar{\bar{l}}}$ und, setzt man $\bar{l} - \bar{\bar{l}} = \bar{e}$, so zerfällt das Primideal $\mathfrak{p}_{\bar{v}}$ beim Übergange von dem einmal- zum zweimal überstrichenen Verzweigungskörper nach der Formel

$$\mathfrak{p}_{\bar{v}} = (\mathfrak{p}_{\bar{\bar{v}}})^{p^{\bar{e}}}$$

in $p^{\bar{e}}$ gleiche Primideale f^{ten} Grades des Körpers $\mathfrak{k}_{\bar{\bar{v}}}$; zudem ist die Erzeugende $\bar{\bar{\eta}}$ dieses Körpers durch eine in $\mathfrak{k}_{\bar{v}}$ irreduktible Gleichung vom Grade $p^{\bar{e}}$ bestimmt, welche relativ zu $\mathfrak{k}_{\bar{v}}$ eine Abelsche Gleichung ist.

In derselben Weise wird man zu dreifach oder noch mehrfach überstrichenen Verzweigungskörpern geführt werden, bei denen vom einen zum andern jedesmal eine weitere Zerlegung des Primidealfaktors von p stattfindet. Da aber jeder dieser successiven Körper ein Oberkörper des voraufgehenden, sein Grad also ein Vielfaches vom Grade des letzteren ist, so muß schließlich einer dieser Körper mit dem Körper $\mathfrak{K}$ selbst identisch werden, somit der Prozeß sich schließen und das Ideal $\mathfrak{P}$ selbst als Primidealfaktor von p erscheinen. Der Umstand, daß der Grad N der Gesamtgruppe G ein Vielfaches ist vom Grade jeder ihrer Untergruppen, die Grade der Verzweigungsgruppen aber Potenzen von p sind, läßt ferner erkennen, daß, falls N durch p nicht aufgeht, jedenfalls keine überstrichenen Verzweigungsgruppen und -körper vorhanden sein können, ein Verzweigungskörper $\mathfrak{k}_v$ aber nur dann, wenn $r_v = p^l = 1$, d. h. wenn die Gruppe g_v nur aus der identischen Substitution besteht, der Verzweigungskörper $\mathfrak{k}_v$ also mit dem Galoisschen Körper $\mathfrak{K}$ selbst identisch ist. Allgemeiner wird diese Identität eintreten auch in dem Falle, wo zwar N aufgeht durch p, aber der Grad r_t der Trägheitsgruppe durch p nicht teilbar ist, da wegen $r_t = hr_v = h \cdot p^l$ dann $p^l = 1$ sein

muß. Ist aber r_t teilbar durch p, so lehrt dieselbe Beziehung, in welcher h nicht aufgeht durch p, daß $r_v = p^j > 1$ ist; in diesem Falle ist $\mathfrak{k}_v$ noch ein von $\mathfrak{K}$ verschiedener Unterkörper und somit mindestens noch ein — möglicherweise mit $\mathfrak{K}$ bereits zusammenfallender — überstrichener Verzweigungskörper vorhanden.

Ferner ersieht man aus den erhaltenen Sätzen über die Gleichungen, durch welche die Erzeugenden der aufeinanderfolgenden Körper bestimmt sind, daß die den Galoisschen Körper erzeugende ganze Zahl A einer in bezug auf den in der Reihe nächst vorhergehenden Unterkörper Abelschen Gleichung oder, falls $\mathfrak{K}$ mit dem Verzweigungs- oder gar mit dem Trägheitskörper identisch ist, einer in bezug auf $\mathfrak{k}_t$ resp. $\mathfrak{k}_z$ zyklischen Gleichung genügt; dabei ist der Grad jener Abelschen Gleichung eine Potenz von p; demnach ist bekanntlich A durch die Erzeugende des vorangehenden Unterkörpers mittels Wurzelgrößen ausdrückbar. Die Erzeugende dieses Körpers ist es aber in gleicher Weise durch diejenige des nächst vorhergehenden Unterkörpers usw., sodaß man schließlich die Erzeugende A des Galoisschen Körpers durch diejenige des Zerlegungskörpers lediglich mittels Wurzelausziehungen bestimmt findet. Wir sprechen mit Hilbert das so gewonnene Resultat in folgendem Satze aus:

Der Zerlegungskörper eines jeden Primideals im *Galois*schen Körper ist ein Rationalitätsbereich, in welchem die Zahlen des *Galois*schen Körpers lediglich durch Wurzelausdrücke darstellbar sind.

Dieser elegante Satz bietet neben der großen Wichtigkeit, die ihm mit Bezug auf die algebraische Auflösung der Gleichungen zukommt, besonders dadurch ein hohes Interesse dar, daß darin die so innige Beziehung zwischen Algebra und Zahlentheorie, welche zuerst durch Gauss' klassische Arbeiten über die Kreisteilung aufgedeckt worden ist, aufs neue in ausgezeichnetster Weise zutage tritt. In der Tat zeigt der Satz, daß gerade diejenigen Körper, welche für die gradweise fortschreitende Zerlegung von p in Primidealfaktoren von Bedeutung sind, zugleich auch die geeigneten sind, um die alge-

braische Auflösung der den Galoisschen Körper bestimmenden Gleichung zu leisten.

13. Die betrachtete Reihe in einander geschachtelter Unterkörper des Galoisschen Körpers $\mathfrak{K}$ gewährt endlich auch das Mittel, die genaue Potenz des Primideals $\mathfrak{P}$ sowie der Primzahl p festzustellen, welche in seiner Differente resp. Diskriminante aufgeht. Hierzu führen die folgenden Sätze:

1) Die Differente des Trägheitskörpers ist durch das Primideal $\mathfrak{P}$ nicht teilbar. Sind nämlich $\omega_1, \omega_2, \omega_3, \ldots$ eine Basis für die Gesamtheit der ganzen Zahlen in $\mathfrak{k}_t$, so sind „die Elemente“ von $\mathfrak{k}_t$ solche, dem Galoisschen Körper angehörige Ideale

$$\{\omega_1 - s\omega_1, \; \omega_2 - s\omega_2, \; \omega_3 - s\omega_3, \; \cdots\},$$

in denen s eine nicht zur Trägheitsgruppe gehörige Substitution des Galoisschen Körpers bezeichnet. Ein solches Element und damit die Differente von $\mathfrak{k}_t$ könnte aber nur dann durch $\mathfrak{P}$ teilbar sein, wenn jede der Differenzen $\omega_i - s\omega_i$ und daher auch für jede Zahl ω in $\mathfrak{k}_t$ die Differenz $\omega - s\omega$ durch $\mathfrak{P}$ teilbar wäre. Ist dann also ω irgend eine Zahl des in $\mathfrak{k}_t$ liegenden Primideals $\mathfrak{p}_t = \mathfrak{P}^{r_t}$, mithin in $\mathfrak{P}$ enthalten, so gilt das gleiche von $s\omega$ und somit ist $s\mathfrak{p}_t = (s\mathfrak{P})^{r_t}$ teilbar durch $\mathfrak{P}$, was die Gleichheit von $\mathfrak{P}$ und $s\mathfrak{P}$ zur Folge hat. Nun ist nach Nr. 9 jede ganze Zahl Ω des Galoisschen Körpers einer Zahl ω in $\mathfrak{k}_t$ (mod. $\mathfrak{P}$) kongruent:

$$\Omega \equiv \omega \pmod{\mathfrak{P}}.$$

Da hieraus dem eben Bemerkten zufolge

$$s\Omega \equiv s\omega \pmod{\mathfrak{P}}$$

geschlossen wird, so ergibt sich für jede ganze Zahl Ω des Galoisschen Körpers die Kongruenz

$$s\Omega \equiv \Omega \pmod{\mathfrak{P}},$$

welche der Annahme, daß die Substitution s nicht zur Trägheitsgruppe gehört, zuwiderläuft und demnach die Aussage des Satzes bestätigt.

2) Die Relativdifferente des Verzweigungskörpers $\mathfrak{k}_v$ in bezug auf den Trägheitskörper $\mathfrak{k}_t$ ist durch $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$, aber durch keine höhere Potenz von $\mathfrak{P}$

teilbar. Bezeichnen nämlich jetzt $\omega_1, \omega_2, \omega_3, \cdots$ eine Basis aller ganzen Zahlen des Verzweigungskörpers, so ist jedes als Faktor der genannten Relativdifferente auftretende Element von $\mathfrak{k}_v$ ein im Galoisschen Körper enthaltenes Ideal

$$(91) \qquad \{\omega_1 - \tau\omega_1,\ \omega_2 - \tau\omega_2,\ \omega_3 - \tau\omega_3,\ \cdots\},$$

in welchem τ jede der nicht der Verzweigungsgruppe angehörigen Substitutionen t^m der Gruppe g_t ist. Nun ist für jede Zahl ω des Verzweigungskörpers zunächst $\omega - \tau\omega$ in $\mathfrak{P}$ enthalten, andererseits aber auch eine Zahl in $\mathfrak{k}_v$, da für jede Substitution v der Verzweigungsgruppe eine andere v' derselben so angebbar ist, daß $t^m v' = v t^m$, mithin

$$v(\omega - t^m\omega) = v\omega - t^m v'\omega = \omega - t^m\omega,$$

d. h. $\omega - t^m\omega$ bei jeder Substitution der Verzweigungsgruppe unveränderlich ist. Demnach ist $\omega - t^m\omega$ auch eine Zahl im Ideale $\mathfrak{p}_v = \mathfrak{P}^{r_v}$, welches die Gesamtheit aller zugleich in $\mathfrak{P}$ und in $\mathfrak{k}_v$ enthaltenen Zahlen darstellt und folglich ist $\omega - t^m\omega$ teilbar durch $\mathfrak{P}^{r_v}$. Hiernach wird jedes der Elemente (91) mindestens durch die Potenz $\mathfrak{P}^{r_v}$ teilbar sein. Keins derselben geht aber durch eine höhere Potenz von $\mathfrak{P}$ auf. Denn andernfalls müßten sämtliche Differenzen $\omega_i - t^m\omega_i$ und daher auch für jede in $\mathfrak{k}_v$ enthaltene Zahl ω die Differenz $\omega - t^m\omega$ durch $\mathfrak{P}^{r_v+1}$ aufgehen; man kann aber eine solche Zahl angeben, für welche dies nicht der Fall ist. In der Tat, sei ω eine durch $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ aber nicht durch $\mathfrak{p}_v^2$ teilbare Zahl in $\mathfrak{k}_v$ und P die in Nr. 10 eingeführte durch $\mathfrak{P}$ aber nicht durch $\mathfrak{P}^2$ teilbare Zahl des Galoisschen Körpers, P die ebenfalls dort benutzte Primitivzahl (mod. $\mathfrak{P}$). Setzt man dann

$$\omega = \mathfrak{P}^{r_v} \cdot \mathfrak{Q}, \quad P = \mathfrak{P} \cdot \mathfrak{A},$$

wo $\mathfrak{A}$, $\mathfrak{Q}$ Ideale sind, welche durch $\mathfrak{P}$ nicht aufgehen, sodaß

$$\mathfrak{A}^{r_v} \cdot \omega = P^{r_v} \cdot \mathfrak{Q}$$

hervorgeht, so ergibt sich durch eine Betrachtung, welche der an die Formel (72) geknüpften völlig analog ist, die nachstehende Kongruenz:

$$\left.\begin{aligned} &\omega \equiv P^{r_v} \cdot Q \\ \text{oder} \\ (92) \qquad &\omega \equiv P^{r_v} \cdot \mathrm{P}^u \end{aligned}\right\} (\text{mod. } \mathfrak{P}^{r_v+1}),$$

worin u eine der Zahlen $0, 1, 2, \cdots, p^f - 2$. Nun kann für die zu g_t aber nicht zu g_v gehörige Substitution t^m

$$t^m P \equiv \mathrm{P}^\alpha \cdot P \pmod{\mathfrak{P}^2}$$

gesetzt werden, unter α eine der Zahlen

$$(93) \qquad a,\ 2a,\ 3a, \cdots, (h-1)a$$

verstanden; mit Rücksicht auf (92) ergibt sich daher leicht

$$t^m \omega \equiv \mathrm{P}^{r_v} \cdot \mathrm{P}^{u + \alpha r_v} \equiv \omega \cdot \mathrm{P}^{\alpha r_v} \pmod{\mathfrak{P}^{r_v + 1}},$$

also

$$\omega - t^m \omega \equiv \omega\,(1 - \mathrm{P}^{\alpha r_v}) \pmod{\mathfrak{P}^{r_v + 1}}.$$

Dieser Kongruenz zufolge kann $\omega - t^m \omega$ nicht durch $\mathfrak{P}^{r_v + 1}$ teilbar sein, da sonst $1 - \mathrm{P}^{\alpha r_v}$ durch $\mathfrak{P}$ aufgehen, also αr_v ein Vielfaches von $p^f - 1$ sein müßte, was doch nicht sein kann, da $r_v = p^l$ prim gegen $p^f - 1$ und α als eine der Zahlen (93) kleiner als $p^f - 1 = ha$ ist.

Aus alle diesem geht hervor, daß jedes der $h - 1$ Elemente (91), aus denen die Relativdifferente von $\mathfrak{k}_v$ bezüglich $\mathfrak{k}_t$ durch Multiplikation entsteht, genau durch $\mathfrak{P}^{r_v}$ und somit die Relativdifferente selbst genau durch $\mathfrak{P}^{(h-1) r_v} = \mathfrak{P}^{r_t - r_v}$ teilbar ist, wie der Satz es behauptet.

3) In ganz analoger Weise erkennt man die Richtigkeit der entsprechenden Sätze: Die Relativdifferente von $\mathfrak{k}_{\bar v}$ bezüglich $\mathfrak{k}_v$ ist genau teilbar durch $\mathfrak{P}^{\lambda (r_v - r_{\bar v})} = \mathfrak{p}_{\bar v}^{\lambda (p^{\bar f} - 1)}$, diejenige von $\mathfrak{k}_{\bar{\bar v}}$ bezüglich $\mathfrak{k}_{\bar v}$ genau durch $\mathfrak{P}^{\bar\lambda (r_{\bar v} - r_{\bar{\bar v}})} = \mathfrak{p}_{\bar v}^{\bar\lambda (p^{\bar{\bar f}} - 1)}$, usw. fort.

Verbindet man die in diesen Sätzen enthaltenen Resultate mit der Formel (36) des 11. Kapitels, so leuchtet sogleich die Wahrheit des folgenden Satzes ein:

Die Differente des *Galois*schen Körpers enthält genau die Potenz $\mathfrak{P}^m$, wo

$$(94) \qquad m = r_t - r_v + \lambda (r_v - r_{\bar v}) + \bar\lambda (r_{\bar v} - r_{\bar{\bar v}}) + \cdots$$

gesetzt ist

Und da nach Nr. 4 die Diskriminante D des Galoisschen Körpers gleich der N^{ten} Potenz der Differente ist, also den Primfaktor $\mathfrak{P}$ genau Nm Mal enthält, andererseits nach (41) jeder Primfaktor p, so oft er in D aufgeht, den Primfaktor $\mathfrak{P}$

je r_t Mal in D einführt, so geht p offenbar μ Mal in D auf, wenn

$$\mu \cdot r_t = Nm,$$

d. h.

$$\mu = n_t \cdot m$$

gesetzt wird. Die Diskriminante des *Galois*schen Körpers enthält demnach den Primfaktor p genau in der μ^{ten} Potenz, wenn

$$(95) \qquad \mu = n_t[r_t - r_v + \lambda(r_v - r_{\bar{v}}) + \bar{\lambda}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots]$$

gesetzt wird.

Nach dem allgemeinen Satze in Nr. 13 des 7. Kapitels geht D mindestens auf durch die Potenz

$$(96) \qquad p^{f_1(e_1 - 1) + f_2(e_2 - 1) + \cdots},$$

wenn die Zerlegung von p in Primidealfaktoren

$$p = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdots$$

ist und die Primideale $\mathfrak{P}_1, \mathfrak{P}_2, \cdots$ resp. von den Graden $f_1, f_2, \cdots$ sind; die Potenz (96) ist zugleich die höchste in D aufgehende, wenn keiner der Exponenten e_i durch p teilbar ist. Hier ist nach (41) $e_i = r_t$ und die Anzahl der Primideale $\mathfrak{P}_i$, welche sämtlich f^{ten} Grades sind, gleich n_z. Ist demnach r_t nicht teilbar durch p, so muß μ mit dem Exponenten in (96) identisch sein. In der Tat sind unter solcher Voraussetzung keine überstrichenen Verzweigungskörper vorhanden und $\mathfrak{k}_v$ mit dem Galoisschen Körper identisch, also ist $r_v = 1$, $\mu = n_t(r_t - 1)$, ein Wert, welcher mit dem Exponenten von (96), nämlich

$$N - n_z \cdot f = N - f \cdot \frac{N}{r_z} = N - \frac{N}{r_t}$$

übereinkommt. Dieser Fall ereignet sich notwendig, so oft der Grad N des Galoisschen Körpers durch p nicht aufgeht.

14. Wir beendigen diesen Abschnitt mit einer interessanten Bemerkung, welche Minkowski[1]) bezüglich der Einheiten im Galoisschen Körper gemacht hat. Da nämlich die Konjugierten einer Zahl dieses Körpers stets zu eben demselben Körper gehören, so sind die Konjugierten jeder Einheit

1) Minkowski, Göttinger Nachr. 1900, p. 90.

des Galoisschen Körpers ebenfalls Einheiten desselben, und es liegt nahe, die Frage aufzuwerfen, ob die $s-1$ unabhängigen Einheiten, aus denen nach *Dirichlets* allgemeinem Satze alle Einheiten eines Körpers zusammensetzbar sind, im *Galois*schen Körper etwa als unter einander konjugierte Einheiten gewählt werden können. *Minkowski* hat gezeigt, daß dies in der Tat möglich ist.

Da jede Wurzel der den Galoisschen Körper erzeugenden Gleichung (1) eine rationale Funktion einer beliebigen ihrer Wurzeln mit rationalen Koeffizienten ist, so sind entweder alle Wurzeln reell oder sie sind paarweise konjugiert imaginär; die in der Theorie der Einheiten mit s bezeichnete Zahl ist also entsprechend gleich N oder gleich $\frac{N}{2}\cdot$ Es seien im ersteren Falle

$$\text{(97)} \qquad A_1,\ A_2,\ \cdots,\ A_s$$

sämtliche Wurzeln von (1), im letzteren Falle je eine Wurzel aus jedem der Paare konjugiert imaginärer Wurzeln; die den Galoisschen Körper erzeugende Zahl A befindet sich im erstern Falle von selbst unter den Wurzeln (97), im zweiten soll es vorausgesetzt werden. Dann gelten Gleichungen von der Form

$$A_h = f_h(A), \quad A = \varphi_h(A_h), \qquad (h = 1, 2, \cdots, s)$$

wo f_h, φ_h rationale Funktionen bedeuten, und aus ihnen folgt

$$\varphi_h(f_h(A)) = A,$$

also wegen der Irreduktibilität der Gleichung (1) allgemein auch

$$\text{(98)} \qquad \varphi_h(f_h(A_k)) = A_k. \qquad (h, k = 1, 2, \cdots, s)$$

Da ferner $f_h(A)$ eine Wurzel der irreduktibeln Gleichung (1) ist, so ist's auch $f_h(A_k)$, und demnach sind

$$\text{(99)} \qquad f_h(A_1),\ f_h(A_2),\ \cdots,\ f_h(A_s)$$

s Konjugierte zu A; zudem sind keine zwei von ihnen einander gleich oder konjugiert imaginär, da, wenn es $f_h(A_k)$, $f_h(A_l)$ wären, auch

$$\varphi_h(f_h(A_k)), \quad \varphi_h(f_h(A_i)),$$

d. h. A_k, A_i es sein müßten, der Wahl der Werte (97) zuwider. Demnach müssen die absoluten Beträge der Größen (99) von der Reihenfolge abgesehen denen der Größen (97) gleich sein.

Dies vorausgeschickt, sei ε eine Einheit des Galoisschen Körpers, welche als eine Zahl dieses Körpers einer rationalen Funktion von A gleichgesetzt werden kann, etwa

$$\varepsilon = \psi(A).$$

Dann sind

$$\varepsilon_1 = \psi(A_1), \quad \varepsilon_2 = \psi(A_2), \cdots, \quad \varepsilon_s = \psi(A_s)$$

die Konjugierten von ε, welche den Werten (97) entsprechen. Nun ist aber

$$\varepsilon_h = \psi(A_h) = \psi(f_h(A))$$

auch eine Einheit des Galoisschen Körpers und

$$\text{(100)} \qquad \psi(f_h(A_1)), \quad \psi(f_h(A_2)), \cdots, \quad \psi(f_h(A_s))$$

die den Werten (97) entsprechenden Konjugierten derselben, und nach dem bezüglich der Größen (97) und (99) Gesagten müssen die absoluten Beträge dieser Konjugierten von der Reihenfolge abgesehen denjenigen der Konjugierten $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_s$ gleich sein. Nun wähle man die Einheit ε so, was nach Dirichlets Theorie möglich ist, daß diejenige der Konjugierten, welche gleich $\psi(A)$ ist, einen absoluten Betrag größer, alle übrigen einen absoluten Betrag kleiner als Eins haben; dann wird auch für die Einheit ε_h eine einzige der Konjugierten, nämlich diejenige Zahl der Reihe (100), in welcher $f_h(A_i)$ gleich oder konjugiert imaginär mit A, d. h. A_i mit $\varphi_h(A)$ ist, dem absoluten Betrage nach größer, alle übrigen kleiner als Eins sein, und für die verschiedenen Werte $h = 1, 2, \cdots, s$ wird die erstbezeichnete Konjugierte jedesmal einer anderen der Größen (97) entsprechen, da dasselbe A_i nicht mit zweien der Größen

$$\varphi_1(A), \quad \varphi_2(A), \cdots, \quad \varphi_s(A)$$

gleich oder konjugiert imaginär sein kann. Hieraus geht hervor, daß je $s-1$ unter den konjugierten Einheiten

$$\varepsilon_1, \; \varepsilon_2, \cdots, \; \varepsilon_s$$

genau solche $s-1$ Einheiten des Galoisschen Körpers sind,

wie sie in Kap. 8, Nr. 5 als ein „System von unabhängigen Einheiten" nachgewiesen worden sind, und somit ergibt sich mit Rücksicht auf Nr. 9 desselben Kapitels der Satz:

Im *Galois*schen Körper gibt es stets eine *solche* Einheit, daß *jede* Einheit dieses Körpers als ein Produkt aus Potenzen der ersteren und ihrer Konjugierten mit rationalen Exponenten darstellbar ist.

Anhang.

Reihenentwicklung der Zahlen.

Hiermit wären die hauptsächlichsten Fragen der allgemeinen Arithmetik der Zahlenkörper, soweit sie bisher behandelt worden sind, im wesentlichen zur Darstellung gekommen und wir könnten unser Werk schließen. Indessen würde es doch der wünschenswerten Vollständigkeit ermangeln, wenn wir nicht der neuesten Theorie der algebraischen Zahlen, welche von Hensel herrührt[1]) und auf einer von der bisher ent-

1) Eine noch andere Theorie der algebraischen Zahlen, welche J. Sochotzki zum Verfasser hat (Das Prinzip des größten gemeinsamen Teilers in seiner Anwendbarkeit auf die Teilbarkeit algebraischer Zahlen, russisch und polnisch, 1893), ist mir nur nach dem bezüglichen Berichte im Jahrb. üb. die Fortschritte der Math. 1893 bekannt. Diesem zufolge ist ihr die Begründung auf einen gewissen Euklidischen Algorithmus eigentümlich. Man nenne a die Ordnung von α (mod. p), wenn $N(\alpha) = p^a \cdot h$, h durch p nicht teilbar ist, nenne ferner α relativ prim zu p, wenn $a = 0$. Ist γ relativ prim zu p und $\frac{\gamma\alpha}{\beta}$ eine ganze Zahl, so heiße α (mod. p) teilbar durch β. Dann gilt als Fundament der Theorie der Satz: Sind α, β zwei von Null verschiedene Zahlen, von denen α nicht (mod. p) teilbar ist durch β, so gibt es eine Zahl ω, für welche die Ordnung $\frac{\alpha}{\beta} - \omega$ (mod. p) kleiner ist als diejenige von $\frac{\alpha}{\beta}$. Dies führt dann zur Bestimmung des größten gemeinsamen Teilers von α, β (mod. p), usw., sowie kraft besonderer weiterer Definitionen auch zu den Sätzen der Teilbarkeit schlechthin, kurz zur gesamten Theorie der algebraischen Zahlen.

wickelten ganz verschiedenen Grundlage beruht, anhangsweise noch Erwähnung täten, und dies darf um so weniger unterbleiben, als dieselbe bereits in bezug auf den allgemeinen Satz von der Zusammensetzung der Grundzahl eines Körpers, auf den wir zuletzt zurückgeführt worden sind, einen wesentlichen Fortschritt über die früheren Resultate herbeigeführt hat. Wir werden uns aber dabei zum Teil auf eine kurze Skizzierung beschränken.

1. Sei $K(\omega)$ ein gegebener Körper n^{ten} Grades und $\omega_1, \omega_2, \cdots, \omega_n$ die ihn erzeugende Zahl ω mit ihren Konjugierten. In diesem Körper sei

$$(1) \qquad p = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \mathfrak{p}_3^{e_3} \cdots$$

die Zerlegung der reellen Primzahl p in ihre Primidealfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \cdots$ von den Graden $f_1, f_2, \cdots$ resp.; es bezeichne $\mathfrak{p}^e$ irgend eine der Primidealpotenzen dieser Zerlegung und f den Grad des Primideals $\mathfrak{p}$. Dann ist analog mit Kap. 6, Nr. 21, insbesondere mit Formel (153) daselbst jede ganze Zahl des Körpers (mod. $\mathfrak{p}^m$) einem eindeutig bestimmten Ausdrucke kongruent von der Form:

$$(2) \qquad A_0 + A_1\pi + A_2\pi^2 + \cdots + A_{m-1}\pi^{m-1},$$

worin π eine zwar durch $\mathfrak{p}$ aber nicht mehr durch $\mathfrak{p}^2$ teilbare ganze Zahl des Körpers und

$$(3) \qquad A_i = a_{i0} + a_{i1}\varrho + a_{i2}\varrho^2 + \cdots + a_{i,f-1}\varrho^{f-1}$$

ist, während die Koeffizienten a_{ik} (mod. p) reduzierte ganze Zahlen und die in $K(\omega)$ enthaltene ganze Zahl ϱ Wurzel einer (mod. p) irreduktibeln Kongruenz

$$(4) \qquad P(x) \equiv 0 \pmod{\mathfrak{p}}$$

vom Grade f ist, deren ganzzahlige Koeffizienten ebenfalls als (mod. p) reduzierte Zahlen gedacht werden dürfen. Dies überträgt sich auch auf jede gebrochene Zahl des Körpers, nur daß für eine solche die Entwicklung (2) mit negativen Potenzen von π beginnen kann, und somit gilt für jede Zahl ζ des Körpers und für einen beliebig großen Wert des Exponenten m die Kongruenzbeziehung

$$(2^a) \qquad \zeta \equiv A_r\pi^r + A_{r+1}\pi^{r+1} + A_{r+2}\pi^{r+2} + \cdots \pmod{\mathfrak{p}^m},$$

wo der Exponent r, der die **Ordnung** von ζ (mod. $\mathfrak{p}$) heiße, eine ganze Zahl ist, welche Null, positiv oder negativ sein kann, und man die rechte Seite fortzusetzen hat, so lange der Exponent von π den Wert m nicht erreicht.

Offenbar darf hierbei die Zahl ϱ durch irgend einen ihr (mod. $\mathfrak{p}$) kongruenten ganzzahligen Ausdruck

$$\bar{\varrho} = \varrho + a_1\pi + a_2\pi^2 + \cdots \tag{5}$$

und die Zahl π durch jeden ganzzahligen Ausdruck

$$\bar{\pi} = b_1\pi + b_2\pi^2 + \cdots \tag{6}$$

ersetzt werden, in welchem b_1 prim gegen p ist. Diese Wahrheit nutzen wir zunächst zur Bestimmung einer neuen Zahl $\bar{\varrho}$, welche die Kongruenz (4) nicht nur (mod. $\mathfrak{p}$), sondern nach jeder beliebig hohen Potenz $\mathfrak{p}^m$ als Modulus befriedigt. Man bemerke zuvörderst, daß für eine Zahl ϱ, welche die Kongruenz (4) erfüllt, nicht auch

$$P'(\varrho) \equiv 0 \pmod{\mathfrak{p}}$$

sein kann, denn die (mod. p) irreduktible Funktion $P(x)$ ist nach Kap. 3, Nr. 3 prim gegen $P'(x)$ (mod. p), mithin besteht eine Kongruenz

$$P(x)\,\varphi(x) + P'(x)\,\psi(x) \equiv 1 \pmod{p}$$

also auch (mod. $\mathfrak{p}$), welche zeigt, daß nicht gleichzeitig $P(x)$, $P'(x)$ für $x = \varrho$ durch $\mathfrak{p}$ teilbar sein können. Dies vorausgeschickt, sei $\bar{\varrho}$ bereits so gewählt, daß $P(\bar{\varrho})$ genau durch $\mathfrak{p}^l$ teilbar, also von der Form

$$C_l\pi^l + C_{l+1}\pi^{l+1} + \cdots$$

sei, wo $l \geqq 1$. Dann ist, wenn $\bar{\varrho}$ durch $\bar{\varrho} + A\pi^l$ ersetzt wird,

$$\begin{aligned} P(\bar{\varrho} + A\pi^l) &= P(\bar{\varrho}) + A\pi^l \cdot P'(\bar{\varrho}) + \cdots \\ &= \pi^l(C_l + AP'(\bar{\varrho})) + \cdots \end{aligned}$$

und wird daher, wenn die Zahl A, was dem zuvor Bemerkten zufolge geschehen kann, der Kongruenz

$$C_l + AP'(\bar{\varrho}) \equiv 0 \pmod{\mathfrak{p}}$$

gemäß gewählt wird, gewiß durch $\mathfrak{p}^{l+1}$ teilbar; und da man, ausgehend von ϱ, diese Betrachtung beliebig weit fortsetzen

kann, findet man eine andere Zahl $\bar{\varrho}$ von der Form (5), für welche $P(\bar{\varrho})$ durch eine beliebig hohe Potenz von $\mathfrak{p}$ teilbar ist, w. z. b. w.

Aber auch die Zahl π soll durch eine geeignetere Zahl $\bar{\pi}$ von der Form (6) ersetzt werden. Da π genau durch $\mathfrak{p}$ und p genau durch $\mathfrak{p}^e$ teilbar ist, so wird $\frac{\pi^e}{p}$ von der Ordnung Null (mod. $\mathfrak{p}$) sein, die zugehörige Entwicklung dieses Quotienten (mod. $\mathfrak{p}^m$) also mit der nullten Potenz von π beginnen und somit, wenn die Anfangsglieder der Entwicklung nach links geschafft werden,

$$\frac{\pi^e}{p} + B_{e-1}\pi^{e-1} + B_{e-2}\pi^{e-2} + \cdots + B_0 = B'$$

gesetzt werden dürfen, wo die B_i Zahlen des Rationalitätsbereichs $K(\varrho)$ sind, von denen B_0 gewiß nicht Null, während B' (mod. $\mathfrak{p}$) mindestens von der Ordnung e ist. Demnach findet sich gleicherweise

$$\frac{B'}{p} + B'_{e-1}\pi^{e-1} + B'_{e-2}\pi^{e-2} + \cdots + B_0' = B'',$$

wo B'' wieder mindestens von der Ordnung e ist, also

$$\frac{B''}{p} + B''_{e-1}\pi^{e-1} + B''_{e-2}\pi^{e-2} + \cdots + B_0'' = B''',$$

usw., und aus diesen Beziehungen folgt, wenn

$$(7) \qquad pC_i = pB_i + p^2B_i' + p^3B_i'' + \cdots$$

gesetzt wird, für eine beliebig hohe Potenz von $\mathfrak{p}$ als Modulus die Kongruenz

$$(8) \quad \Phi(\pi) = \pi^e + pC_{e-1}\pi^{e-1} + pC_{e-2}\pi^{e-2} + \cdots + pC_0 \equiv 0,$$

oder: die Zahl π ist Wurzel einer Kongruenz

$$(9) \qquad \Phi(x) \equiv 0 \pmod{\mathfrak{p}^m},$$

deren Koeffizienten durch p teilbare Zahlen pC_i des Rationalitätsbereiches $K(\varrho)$ sind, die letzte von ihnen,

$$pC_0 = pB_0 + p^2B_0' + \cdots,$$

zudem durch keine höhere als die erste Potenz von p teilbar. Nach einem bekannten Satze von Eisenstein (s. des Verf. Lehre von der Kreisteilung etc., p. 36), der sogleich auf den hier

vorliegenden Fall, in welchem die Koeffizienten nicht gewöhnliche, sondern algebraische ganze Zahlen sind, ausgedehnt werden kann, ist demnach die Funktion $\Phi(x)$ (mod. p) im Rationalitätsbereiche $K(\varrho)$ irreduktibel. Je größer nun die Potenz $\mathfrak{p}^m$ gedacht wird, um so weiter schreiten die Potenzreihen im Ausdrucke (7) fort, um so höher steigen also die Werte der Koeffizienten C_i. Aber man kann die Entwicklungszahl π durch eine andere von der Form (6) ersetzen, für welche im Gegenteil die Koeffizienten C_i unter einer endlichen Grenze verbleiben, wie hoch die Potenz $\mathfrak{p}^m$ auch gewählt werde.

Hierzu beachte man, daß die einzelnen Summanden

$$p^h \cdot B_i^{(h-1)} \cdot \pi^i,$$

aus denen sich $\Phi(\pi)$ wegen (7) zusammensetzt, soweit sie wirklich vorhanden sind, in bezug auf $\mathfrak{p}$ von der Ordnung $he+i$ sind, da $B_i^{(h-1)}$, wenn es von Null verschieden, seiner Bedeutung nach durch $\mathfrak{p}$ nicht teilbar ist. Alle diese einzelnen Summanden sind also von verschiedener Ordnung (mod. $\mathfrak{p}$), ausgenommen diese beiden: π^e und pB_0, welche die gleiche Ordnung e haben. Man schließt daraus, daß die abgeleiteten Ausdrücke

$$\frac{\Phi'(\pi)}{1}, \quad \frac{\Phi''(\pi)}{1\cdot 2}, \quad \ldots, \quad \frac{\Phi^{(e)}(\pi)}{1\cdot 2\cdots e} \tag{10}$$

je aus lauter Teilen verschiedener Ordnung bestehen. Was nun $\Phi(\pi)$ selbst betrifft, so denke man sich diejenigen Summanden, deren Ordnung gleich oder kleiner ist als eine sogleich näher zu bestimmende feste Zahl k, zusammengefaßt in den Ausdruck $\Psi(\pi)$, alle übrigen in den Ausdruck $X(\pi)$, sodaß

$$\Phi(\pi) = \Psi(\pi) + X(\pi)$$

und die Summanden von $X(\pi)$ von höherer Ordnung sind als k Aus (8) ergibt sich dann

$$\Psi(\pi) \equiv D_l\pi^l + D_{l+1}\pi^{l+1} + \cdots, \tag{11}$$

worin $l > k$. Setzt man nun $\bar{\pi} = \pi + \lambda\pi^r$, so folgt

$$\begin{aligned} \Psi(\bar{\pi}) &= \Psi(\pi) + \lambda\pi^r \cdot \Psi'(\pi) + \lambda^2\pi^{2r} \cdot \frac{\Psi''(\pi)}{1\cdot 2} + \cdots \\ &\equiv D_l\pi^l + D_{l+1}\pi^{l+1} + \cdots + \lambda\pi^r \cdot \Psi'(\pi) + \cdots \end{aligned} \tag{12}$$

Da die Faktoren der Potenzen von $\lambda\pi^r$ Bestandteile der Ausdrücke (10) sind, gilt von ihnen die für die letztern gemachte Bemerkung und zugleich werden ihre Summanden niedrigster Ordnung in bezug auf $\mathfrak{p}$ die Summanden niedrigster Ordnung auch für jene sein; man nenne

$$\varrho_1, \varrho_2, \cdots, \varrho_e$$

diese Ordnungszahlen resp. In (12) besitzen dann die auf $\Psi(\pi)$ folgenden Glieder die Ordnungszahlen

$$\varrho_1 + r, \quad \varrho_2 + 2r, \cdots, \varrho_e + er.$$

Nun sei r_0 die kleinste ganze Zahl, für welche

$$\varrho_1 + r_0 < \varrho_i + ir_0$$
$$(i = 2, 3, \cdots, e)$$

ist, welche also oberhalb aller Zahlen

$$\frac{\varrho_1 - \varrho_i}{i - 1} \qquad (i = 2, 3, \cdots, e)$$

gelegen ist. Für jede Zahl $r \geqq r_0$ werden dann die Ungleichheiten

$$\varrho_1 + r < \varrho_i + ir$$
$$(i = 2, 3, \cdots, e)$$

umsomehr stattfinden und somit nach (12)

$$(13) \qquad \begin{aligned} \Psi(\bar{\pi}) &= \Psi(\pi) + C\lambda\pi^{r+\varrho_1} + \cdots \\ &\equiv (D_l\pi^l + \cdots) + C\lambda\pi^{r+\varrho_1} + \cdots \end{aligned}$$

gesetzt werden dürfen, wo $C\lambda\pi^{r+\varrho_1}$ das Glied niedrigster Ordnung in $\lambda\pi^r\Psi'(\pi)$ vorstellt, alle folgenden Glieder aber von höherer Ordnung sein werden. Die lediglich durch die Ausdrücke (10) bestimmte Zahl $r_0 + \varrho_1 - 1$ ist eine feste, von der Zerlegung von $\Phi(\pi)$ in die Bestandteile $\Psi(\pi)$, $X(\pi)$ unabhängige Zahl. Nehmen wir sie an Stelle der bisher unbestimmten Zahl k, so wird $l > r_0 + \varrho_1$ und, wenn man $r + \varrho_1 = l$ wählt, die Voraussetzung $r > r_0$ erfüllt sein. Alsdann fängt aber die rechte Seite in (13) mit dem Gliede niedrigster Ordnung

$$(D_l + C\lambda) \cdot \pi^l$$

an, welches, da C durch $\mathfrak{p}$ nicht aufgehen kann, durch geeignete Wahl der Zahl λ innerhalb des Körpers $K(\omega)$ durch π^{l+1} teilbar gemacht werden kann. Da man alsdann aber das

gleiche Verfahren wiederholen kann, ohne den Wert von k zu verändern, lassen sich durch Einführung einer Zahl $\bar{\bar{\pi}} = \bar{\pi} + \lambda' \pi^{r'}$ an Stelle von $\bar{\pi}$ usw. beliebig viel weitere Glieder des Ausdrucks (11) zum Verschwinden bringen, mit anderen Worten: Statt π läßt sich eine Zahl $\bar{\pi}$ von der Form (6) finden von der Beschaffenheit, daß die Kongruenz

$$\Psi(\bar{\pi}) \equiv 0$$

in bezug auf eine beliebig hohe Potenz $\mathfrak{p}^m$ als Modulus erfüllt ist; hier besteht aber die linke Seite nur aus einer durch die Zahl k bestimmten endlichen Anzahl von vornherein feststehender Glieder, wie es zu erreichen beabsichtigt war. Man hat auf solche Weise folgendes Ergebnis gewonnen:

Jede Zahl ζ des Körpers $K(\omega)$ läßt sich in bezug auf eine beliebig hohe Potenz von $\mathfrak{p}$ als Modulus auf eindeutige Weise in die Reihe

$$\zeta \equiv A_r \pi^r + A_{r+1} \pi^{r+1} + \cdots \pmod{\mathfrak{p}^m} \tag{14}$$

entwickeln. Die beiden „Entwicklungszahlen" ϱ, π können so gewählt werden, daß ϱ der Kongruenz

$$P(x) \equiv 0 \pmod{\mathfrak{p}^m}, \tag{15}$$

π aber einer Kongruenz

$$\Psi(x) \equiv 0 \pmod{\mathfrak{p}^m} \tag{16}$$

genügt, in welcher die linke Seite von der Form

$$\Psi(x) = x^e + pC_{e-1}x^{e-1} + \cdots + pC_0 \tag{17}$$

ist, während die Koeffizienten pC_i Ausdrücke von der Gestalt (7) sind, aber, wie groß auch m gedacht werde, nicht über einen festen Grad in bezug auf p steigen, sodaß von einem bestimmten Werte von m an die Kongruenz (16), ebenso wie die Kongruenz (15), unveränderlich bleibt. Da die Zahl π offenbar durch jede ihr (mod. $\mathfrak{p}^m$) kongruente Zahl ersetzt werden kann, darf man sie als durch keins der von $\mathfrak{p}$ verschiedenen, in p aufgehenden Primideale teilbar voraussetzen, indem sie sich durch eine Zahl π' ersetzen ließe, welche mit π (mod. $\mathfrak{p}^m$), nach jedem andern Primfaktor von p mit 1 kongruent ist.

So oft die Zahl e durch p nicht teilbar ist, hat $\Psi(x)$ die einfache Gestalt

$$\Psi(x) = x^e + pB_0,$$

wo B_0 eine durch $\mathfrak{p}$ nicht teilbare Zahl des Körpers $K(\omega)$ bezeichnet. In der Tat ist bei dieser Voraussetzung in

$$\Psi'(\pi) = e\pi^{e-1} + p(e-1)C_{e-1}\pi^{e-2} + \cdots + pC_1$$

das Glied niedrigster Ordnung das erste von der Ordnung $e-1$, da alle folgenden durch p also mindestens durch $\mathfrak{p}^e$ teilbar sind; demnach ist $\varrho_1 = e-1$; in gleicher Weise findet sich für $i > 1$

$$\varrho_i \overset{=}{>} e - i.$$

Da hiernach

$$\frac{\varrho_1 - \varrho_i}{i-1} \overset{=}{<} \frac{(e-1)-(e-i)}{i-1} = 1$$

ist für alle $i = 2, 3, \cdots, e$, so hat man $r_0 = 2$ zu wählen, wo dann $k = r_0 + \varrho_1 - 1 = e$ wird und aus (13) durch das angegebene Verfahren alle Glieder von höherer Ordnung als e, d. h. alle Glieder außer π^e und $p \cdot B_0$ fortgeschafft werden können.

Nur also in dem ganz singulären Falle, in welchem e durch p teilbar ist, was nur für eine endliche Anzahl von Primzahlen p, die kleiner als der Grad des Körpers sind, zutreffen kann, ist möglicherweise die linke Seite der Kongruenz (16) von der allgemeineren Gestalt (17).

2. Was hier mit den Mitteln der Idealtheorie für die beliebig hohe Potenz eines Primidealfaktors $\mathfrak{p}$ der reellen Primzahl p als Modulus erhalten worden ist, läßt sich, wie Hensel zuerst in einer kurzen Notiz „Über eine neue Begründung der Theorie der algebraischen Zahlen“ im Jahresberichte der deutschen Math. Vereinigung, Bd. 6, p. 83 angegeben hat, in ganz analoger Weise, doch unabhängig von der Idealtheorie, auch (mod. p^m) feststellen. Zwei neueste Arbeiten Hensels („Neue Grundlagen der Arithmetik“, und „Über eine neue Begründung der Theorie der algebraischen Zahlen“ im Journ. f. r. u. a. Math. 127, p. 51 und 128, p. 1) stellen seine Theorie ausführlicher dar. Ihre Grundlage bildet die einfache Bemerkung, daß, wie in bezug auf eine Primzahl p jeder positiven ganzen Zahl die Form einer endlichen Potenzreihe

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

mit (mod. p) reduzierten, d. h. der Reihe $0, 1, 2, \cdots, p-1$ angehörigen Koeffizienten gegeben werden kann, so auch jede negative wie jede gebrochene Zahl sich als eine unendliche Reihe dieser Art auffassen läßt, wenn es sich nicht um deren Wert, sondern eben nur um ihren Rest in bezug auf eine beliebig hohe Potenz von p handelt. In diesem Sinne erweitert nun Hensel das Gebiet aller rationalen Zahlen zum Gebiete all' solcher unendlichen Reihen

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

mit beliebig aber bestimmt gegebenen, (mod. p) reduzierten Koeffizienten, entwickelt die arithmetischen Gesetze für derartige „Zahlengrößen" sowie für ganze Funktionen einer Veränderlichen, in die sie als Koeffizienten eingehen, und zeigt dann, daß auch für algebraische Zahlen ähnliche Darstellungsweisen statthaben, wie für die rationalen, und wie aus ihnen auf die Teilbarkeit der Zahlen durch eine ganze oder gebrochene Potenz von p, bezw. durch eine Potenz eines Primidealfaktors geschlossen werden kann. Für jede Zahl ζ eines Körpers $K(\omega)$ gilt nämlich eine Reihenentwicklung von der Form:

$$\zeta = A_r \pi^r + A_{r+1} \pi^{r+1} + \cdots, \tag{18}$$

wo r eine ganze Zahl, die positiv, Null oder negativ sein kann,

$$A_i = a_0 + a_1 \varrho + \cdots + a_{f-1} \varrho^{f-1}$$

aber eine ganze Funktion von der Wurzel ϱ einer (mod. p) irreduktibeln Gleichung f^{ten} Grades

$$P(x) = 0$$

mit (mod. p) reduzierten Koeffizienten bedeutet; endlich bezeichnet π eine Wurzel einer Gleichung

$$\Psi(x) = 0$$

von der Gestalt (17). Für die allermeisten Primzahlen p ist $\pi = p$, demnach die Reihenentwicklung (18) von der Gestalt

$$\zeta = \frac{A_{-h}}{p^h} + \cdots + \frac{A_{-1}}{p} + A_0 + A_1 p + \cdots; \tag{18^a}$$

sie heiße alsdann regulär und es werde gesagt: zur Primzahl p und zum Körper $K(\omega)$ oder kürzer „zur Stelle (p, ω)" ge-

höre eine reguläre Entwicklung von ζ. Nur für die endliche Menge der Primzahlen, die in der Körperdiskriminante aufgehen, ist π eine gewisse Wurzel aus p oder vielmehr einer solchen „assoziiert"; setzt man nämlich dann $\pi = \varpi \cdot \sqrt[e]{p}$, so genügt ϖ einer Gleichung von der Form

$$(19) \qquad \varpi^e + p^{\frac{e-1}{e}} \cdot C_{e-1} \varpi^{e-1} + p^{\frac{e-2}{e}} \cdot C_{e-2} \varpi^{e-2} + \cdots + C_0 = 0$$

und ist mithin eine ganze algebraische Zahl, welche, da C_0 prim gegen p ist, eben wie diese Zahl C_0 als „eine Einheit (mod. p)" anzusehen ist. Die Entwicklung (18) oder, anders geschrieben,

$$(18^b) \qquad \zeta = \frac{A_{-h}}{\pi^h} + \cdots + \frac{A_{-1}}{\pi} + A_0 + A_1 \pi + \cdots$$

schreitet für die gedachten besonderen Primzahlen p also nach ganzen Potenzen von $p^{\frac{1}{e}}$ fort. Da nun $p^{\frac{1}{e}}$ genau e untereinander konjugierte, nur durch Einheitswurzeln e^{ten} Grades unterschiedene Werte repräsentiert, so ergibt diese eine Formel insgesamt einen Komplex von e verschiedenen, zu einander konjugierten Werten der Zahl ζ. Der singulären Stelle (p, ω) entsprechen also e konjugierte Entwicklungen, genau wie in der Theorie der algebraischen Funktionen zu einer singulären Stelle oder einem Verzweigungspunkte eine Anzahl verschiedener Zweige einer Funktion gehören. Aus diesem Grunde werde die Stelle (p, ω) auch hier eine Verzweigungsstelle $e - 1^{\text{ter}}$ Ordnung genannt, sodaß jede reguläre Stelle auch als Verzweigungsstelle nullter Ordnung bezeichnet werden kann.

Da andererseits die Zahl ϱ, welche in den Koeffizienten A_i auftritt, als Wurzel einer Gleichung f^{ten} Grades $P(x) = 0$ f verschiedene Werte haben kann, so stellt jede der Gleichungen (18^a) oder (18^b) genau f verschiedene Entwicklungen bezw. Komplexe von je e Entwicklungen vor, durch welche je f unter einander konjugierte Werte der Zahl ζ gegeben werden. Diese so zusammengehörigen Entwicklungen oder Komplexe von solchen mögen verbundene Entwicklungen oder Entwicklungskomplexe genannt werden.

Die Vergleichung dieser Sätze mit den Resultaten der vorigen Nummer deutet sogleich den Zusammenhang der

Henselschen Theorie mit derjenigen der Ideale an. Jeder Verzweigungsstelle $e-1^{\text{ter}}$ Ordnung nämlich, in welcher f verbundene Komplexe von je e Entwicklungen vorhanden sind, entspricht ein Primidealfaktor $\mathfrak{p}$ von p, dessen Grad f ist und welcher genau e Mal als Faktor in p auftritt; da, wie früher gezeigt worden ist, e nur für solche Primzahlen, die in der Körperdiskriminante aufgehen, größer als 1 ist, sieht man sogleich, warum für alle übrigen Primzahlen die Verzweigungsstelle zu einer regulären wird und die Entwicklung (18^a) stattfinden muß. Die Ordnungszahl der Entwicklung (18) aber, d. h. der positive oder negative oder der Null gleiche Exponent der Potenz π^r, mit der dieselbe beginnt, gibt die genaue Potenz $\mathfrak{p}^r$ des Primideals $\mathfrak{p}$, durch welche die Zahl ζ teilbar, für welche nämlich $\frac{\zeta}{\pi^r}$ noch ganz ist. Es leuchtet ferner von selbst ein, daß jedem andern Primfaktor $\mathfrak{p}'$ von p vom Grade f' und der Häufigkeit e' eine Verzweigungsstelle $e'-1^{\text{ter}}$ Ordnung entsprechen wird, in welcher f' verbundene Komplexe von je e' Entwicklungen von analoger Beschaffenheit wie die Entwicklungen (18^b) vorhanden sind, womit dann zu den vorigen ef konjugierten Werten der Zahl ζ weitere $e'f'$ hinzugefügt werden usw., derart, daß endlich

$$ef + e'f' + e''f'' + \cdots = n$$

wird.

Von den angegebenen Sätzen aus, durch welche die Theorie der algebraischen Zahlen eine völlig analoge Grundlage und Ausgestaltung erhält, wie diejenige der algebraischen Funktionen, hat Hensel in zwei weiteren Arbeiten („Über die Bestimmung der Diskriminante eines algebraischen Körpers" und „Über die Fundamentalgleichung und die außerwesentlichen Diskriminantenteiler eines algebraischen Körpers" in Götting. Nachr. 1897) auf eine außerordentlich einfache Weise die genaue Zusammensetzung der Diskriminante ermittelt und seine früheren die Fundamentalgleichung betreffenden Resultate (vgl. Kap. 7, Nr. 7 u. 8) bestätigt. Auf letztern Punkt brauchen wir nicht nochmals zurückzukommen; indem wir dagegen das auf die Körperdiskriminante bezügliche Resultat, weil es über das bis dahin Erreichte hinausgeht, noch mitteilen wollen,

ziehen wir gleichwohl vor, zu seiner Herleitung uns an die in Nr. 1 benutzte Henselsche Abhandlung[1]) zu halten, welche es im Anschluß an die in diesem Werke dargestellte Idealtheorie, übrigens mit ganz entsprechenden Grundgedanken, wie die vorgenannte Arbeit, gewinnt.

3. Wir kehren zur Nr. 1 zurück und betrachten die Gleichung

$$P(x) = 0, \tag{20}$$

welche (mod. p), um so mehr also schlechthin irreduktibel ist, und nennen

$$\varrho_1, \varrho_2, \cdots, \varrho_f$$

ihre Wurzeln; ferner sei $\Psi_k(x)$ die Funktion, welche aus $\Psi(x)$ hervorgeht, wenn darin ϱ durch ϱ_k ersetzt wird, und

$$\pi_{k1}, \pi_{k2}, \cdots, \pi_{ke} \tag{21}$$

seien die Wurzeln der im Rationalitätsbereiche $K(\varrho_k)$, ebenso wie es von der Funktion $\Psi(x)$ bemerkt worden ist, irreduktibeln Gleichung

$$\Psi_k(x) = 0. \tag{22}$$

Die Gesamtheit aller aus ϱ_1, π_{11} rational gebildeten Zahlen macht einen Körper $K(\pi_{11}; \varrho_1)$ vom Grade ef aus, für welchen die ef Zahlen

$$\varrho_1{}^g \cdot \pi_{11}{}^h \qquad \begin{pmatrix} g = 0, 1, 2, \cdots, f-1 \\ h = 0, 1, 2, \cdots, e-1 \end{pmatrix} \tag{23}$$

eine Basis d. i. ein System rational unabhängiger Zahlen darstellen (Kap. 1, Nr. 10); die Konjugierten dieses Körpers sind die entsprechend gebildeten ef Körper

$$K(\pi_{kh}; \varrho_k) \qquad \begin{pmatrix} k = 1, 2, \cdots, f \\ h = 1, 2, \cdots, e \end{pmatrix}.$$

Wir wählen irgend einen Galoisschen Körper $\mathfrak{K}$, welcher nicht nur diese Konjugierten, sondern auch den Körper $K(\omega)$ in sich enthält, und verstehen unter $\mathfrak{P}$ einen derjenigen Primidealfaktoren von p in $\mathfrak{K}$, durch welchen das Ideal $\mathfrak{p}$ der Nr. 1 teilbar ist. Dann gelten die Kongruenzen, welche dort in be-

1) K. Hensel, über die Entwicklung der algebraischen Zahlen in Potenzreihen, Math. Annal. 55, p. 301.

zug auf den Modulus $\mathfrak{p}^m$ hergeleitet worden sind, um so mehr auch (mod. $\mathfrak{P}^m$); man überzeugt sich aber unschwer, daß die Entwicklungszahl ϱ einer bestimmten der Wurzeln ϱ_k, sowie die Entwicklungszahl π einer bestimmten der Wurzeln (21) für jede noch so hohe Potenz von $\mathfrak{P}$ kongruent gesetzt werden kann, etwa

$$(24) \qquad \varrho \equiv \varrho_1, \ \pi \equiv \pi_{11} \pmod{\mathfrak{P}^m}.$$

Mithin wird dann jede Zahl des Körpers $K(\omega)$ einer Zahl von der Form

$$(25) \qquad A_r \pi_{11}{}^r + A_{r+1} \pi_{11}^{r+1} + \cdots,$$

worin die A_i ganze ganzzahlige Funktionen der Zahl ϱ_1 sind, (mod. $\mathfrak{P}^m$) kongruent, insbesondere die erzeugende ganze Zahl

$$(26) \qquad \omega \equiv \omega^{(0)} \pmod{\mathfrak{P}^m},$$

wo $\omega^{(0)}$ eine bestimmte Zahl von der Form (25) ist. Zugleich wird also jede (ganze) Zahl des Körpers $K(\omega)$ als rationale Funktion $\varphi(\omega)$ von ω der entsprechenden (ebenfalls ganzen) Zahl $\varphi(\omega^{(0)})$ des Körpers $K(\pi_{11}; \varrho_1)$ kongruent, und in diesem Sinne der gesamte Körper $K(\omega)$ auf den Körper $K(\pi_{11}; \varrho_1)$ „abgebildet". Diese Beziehung ist zudem umkehrbar; denn zugleich mit den zu ϱ, π kongruenten Zahlen ϱ_1, π_{11} ist auch jede rational aus diesen gebildete (ganze) Zahl des Körpers $K(\pi_{11}; \varrho_1)$ der ebenso aus ϱ, π gebildeten (ganzen) Zahl des Körpers $K(\omega)$ kongruent.

Wir zeigen zunächst, daß eine Kongruenz von der Form

$$(27) \qquad \sum_{g=0}^{f-1} \sum_{h=0}^{e-1} a_{gh} \varrho_1{}^g \pi_{11}^h \equiv 0 \pmod{\mathfrak{P}^m}$$

oder einfacher eine Kongruenz

$$(28) \quad A_0 + A_1 \pi_{11} + A_2 \pi_{11}{}^2 + \cdots + A_{e-1} \pi_{11}^{e-1} \equiv 0 \pmod{\mathfrak{P}^m},$$

worin die A_i ganze ganzzahlige Funktionen von ϱ_1 sind, nur identisch stattfinden kann, indem nämlich jedes einzelne Glied der Doppelsumme für sich durch den Modulus teilbar ist. Man bestimme, um dies einzusehen, die höchste in allen A_i aufgehende Potenz

von p; enthält sie den Primfaktor $\mathfrak{P}$ öfter als m mal, so besteht die Kongruenz (27) identisch. Andernfalls geht durch Division mit jener höchsten Potenz von p eine Kongruenz von der gleichen Gestalt:

$$(29) \quad A_0' + A_1'\pi_{11} + A_2'\pi_{11}^2 + \cdots + A_{e-1}'\pi_{11}^{e-1} \equiv 0 \pmod{\mathfrak{P}^{m'}}$$

hervor, in der nun aber nicht sämtliche A_i' mehr durch p teilbar sind. Nun folgt aus der Gleichung

$$(30) \quad \pi_{11}^e + p(C_{e-1}\pi_{11}^{e-1} + \cdots + C_0) = 0,$$

welcher π_{11} genügt, daß der Primidealteiler $\mathfrak{P}$ von p auch in π_{11} aufgeht und daß, wenn er genau δ mal darin aufgeht, er genau $e\delta$ mal in p als Faktor enthalten ist, da C_0 relativ prim ist gegen p. Ist also A_h' in der Reihe $A_0', A_1', A_2', \cdots$ der erste nicht mehr durch p teilbare Koeffizient, so wird, wenn $m' \lesseqgtr h\delta$ ist, jedes Glied der Kongruenz (29) für sich durch $\mathfrak{P}^{m'}$ teilbar, die Kongruenz (27) also identisch erfüllt sein. Die entgegengesetzte Annahme $m' > h\delta$ ist aber unzulässig, denn in ihr reduzierte sich die Kongruenz (29), wenn sie $(\mathrm{mod.}\ \mathfrak{P}^{h\delta+1})$ aufgefaßt wird, offenbar auf die einfache Form

$$A_h'\pi_{11}^h \equiv 0 \pmod{\mathfrak{P}^{h\delta+1}},$$

da alle voraufgehenden Glieder durch p also durch $\mathfrak{P}^{e\delta}$, alle folgenden durch π_{11}^{h+1} also durch $\mathfrak{P}^{(h+1)\delta}$ teilbar sind und so fortfallen; hier müßte jedoch, da π_{11}^h nur die Potenz $\mathfrak{P}^{h\delta}$ zum Faktor hat, A_h' durch $\mathfrak{P}$ und folglich wegen der Irreduktibilität (mod. p) der Gleichung (20), der ϱ_1 genügt, auch durch p teilbar sein, was der Voraussetzung widerstreitet.

Hieraus ergibt sich insbesondere, daß die Basiszahlen (23) des Abbildungskörpers ein Fundamentalsystem (mod. p) für ihn bilden, d. h. daß eine Kongruenz

$$(31) \quad \sum_{g=0}^{f-1}\sum_{h=0}^{e-1} a_{gh}\varrho_1^g\pi_{11}^h \equiv 0 \pmod{p}$$

mit rationalen oder ganzzahligen Koeffizienten oder einfacher eine Kongruenz

$$(32) \quad A_0 + A_1\pi_{11} + A_2\pi_{11}^2 + \cdots + A_{e-1}\pi_{11}^{e-1} \equiv 0 \pmod{p},$$

in welcher die A_i ganze, ganzzahlige Funktionen von ϱ_1 vom

Grade $f-1$ sind, nicht anders möglich ist, als wenn die Koeffizienten a_{gh} oder A_i sämtlich durch p teilbar sind. Denn die Kongruenz (32) liefert die folgende:

$$(32^a) \quad A_0 + A_1\pi_{11} + A_2\pi_{11}^2 + \cdots + A_{e-1}\pi_{11}^{e-1} \equiv 0 \pmod{\mathfrak{P}^{e\delta}},$$

welche erfordert, daß jedes einzelne Glied durch $\mathfrak{P}^{e\delta}$, jeder Koeffizient A_i also sicher durch $\mathfrak{P}$ und deshalb auch durch p teilbar ist.

Auf Grund dieser beiden Sätze erschließt man, daß die Zahl $\omega^{(0)}$ — wenigstens für hinreichend große Werte von m — von demselben Grade ef ist, wie der Abbildungskörper, dem sie angehört. Wir denken $m \gtreqless e\delta$ und nennen

$$(33) \qquad \psi(x) \equiv 0 \pmod{\mathfrak{P}^{e\delta}}$$

die ganzzahlige Kongruenz niedrigsten Grades, der $\omega^{(0)}$ genügt; ihr Grad ν kann nicht größer sein, als der Grad von $\omega^{(0)}$ d. i. als der Grad der ganzzahligen irreduktibeln Gleichung

$$(34) \qquad f(x) = 0,$$

der sie genügt, denn aus der Gleichung $f(\omega^{(0)}) = 0$ ergäbe sich auch die Kongruenz $f(\omega^{(0)}) \equiv 0 \pmod{\mathfrak{P}^{e\delta}}$. Es kann aber gezeigt werden, daß ν nicht kleiner ist als ef, und somit kann auch der Grad der Gleichung (34) nicht kleiner als ef sein, und muß, da er auch nicht größer ist als der Grad ef des Abbildungskörpers, gleich ef sein. Nehmen wir zum Beweise $\nu < ef$ an. Da jede der Zahlen (23) (mod. $\mathfrak{P}^m$) also auch (mod. $\mathfrak{P}^{e\delta}$) einer ganzen Zahl $\varphi(\omega)$ des Körpers $K(\omega)$, mithin auch der entsprechenden Zahl $\varphi(\omega^{(0)})$ des Abbildungskörpers kongruent ist, so ergibt sich mittels der Identität

$$\psi(\omega^{(0)}) \equiv 0 \pmod{\mathfrak{P}^{e\delta}}$$

für jede jener Zahlen eine Beziehung von der Gestalt

$$\varrho_1{}^g \pi_{11}^h \equiv \alpha + \alpha_1 \omega^{(0)} + \cdots + \alpha_{\nu-1} \omega^{(0)^{\nu-1}} \pmod{\mathfrak{P}^{e\delta}}$$

mit rationalen Koeffizienten. Heißt n_{gh} der Generalnenner der letzteren, sodaß allgemein $\alpha_i = \frac{a_i}{n_{gh}}$ gesetzt werden kann, unter den a_i ganze Zahlen verstanden, die nicht sämtlich denselben Teiler mit n_{gh} gemein haben, so kann n_{gh} nicht teilbar sein durch p, da sonst in der Kongruenz

$$(35)\qquad n_{gh}\cdot\varrho_1^g\pi_{11}^h\equiv a+a_1\omega^{(0)}+\cdots+a_{\nu-1}\omega^{(0)^{\nu-1}}\pmod{\mathfrak{P}^{e\delta}}$$

die linke Seite durch $\mathfrak{P}^{e\delta}$ aufginge, $\omega^{(0)}$ also einer Kongruenz von geringerem Grade als ν genügte, ohne daß sämtliche Koeffizienten a_i durch p oder durch $\mathfrak{P}^{e\delta}$ teilbar wären. Ergäbe sich nun aus diesen ef Kongruenzen durch Elimination von $\omega^{(0)}$ eine nicht identische Kongruenz von der Art (27) oder (28), so würde, da eine solche als unmöglich erwiesen ist, sich die Unzulässigkeit der Annahme $\nu < ef$ herausstellen. Eine solche Kongruenz ergibt sich aber in der Tat. Man betrachte nach Belieben ν der gedachten ef Kongruenzen; ihre Determinante Δ kann nicht durch $\mathfrak{P}$ oder als rationale ganze Zahl nicht durch p teilbar sein, denn sonst ließen sich ν durch p nicht sämtlich teilbare ganze Zahlen $c_1, c_2, \cdots, c_\nu$ so angeben, daß die Summe der mit ihnen multiplizierten rechten Seiten jener ν Kongruenzen durch p also durch $\mathfrak{P}^{e\delta}$ aufginge, und da ihr die Summe der mit den c_i multiplizierten linken Seiten (mod. $\mathfrak{P}^{e\delta}$) kongruent ist, würde auch diese Summe durch $\mathfrak{P}^{e\delta}$ teilbar sein, woraus eine Kongruenz von der Form (32ª) hervorginge, ohne daß deren sämtliche Koeffizienten durch p teilbar wären. Da hiernach Δ prim ist gegen $\mathfrak{P}$ und aus jenen ν Kongruenzen jedes der Produkte $\Delta\cdot\omega^{(0)^h}$, folglich nach Multiplikation mit dem Socius von Δ (mod. p) jede Potenz $\omega^{(0)^h}$ einer linearen ganzzahligen Funktion der gedachten ν Zahlen $n_{gh}\varrho_1^g\pi_{11}^h$ (mod. $\mathfrak{P}^{e\delta}$) kongruent wird, so ergibt die Substitution in eine $\nu+1^{\text{te}}$ der Kongruenzen (35) auch für die entsprechende Zahl $n_{gh}\varrho_1{}^g\pi_{11}^h$ ein gleiches, während die einzelnen Summanden des bezüglichen linearen Ausdrucks nicht sämtlich durch $\mathfrak{P}^{e\delta}$ teilbar sind, da diese Zahl $n_{gh}\varrho_1{}^g\pi_{11}^h$ es nicht ist. Somit läge in der Tat eine nicht identische Kongruenz von der Art der Kongruenz (27) vor, w. z. b. w.

4. Da in jedem Körper die Diskriminante eines Fundamentalsystems (mod. p), was ihre Teilbarkeit durch p anbelangt, mit der Diskriminante oder der Grundzahl des Körpers äquivalent ist (s. Kap. 11, Nr. 7), so wird die Diskriminante der Zahlen (23) durch genau dieselbe Potenz von p teilbar sein, wie die Grundzahl des Abbildungskörpers $K(\pi_{11};\varrho_1)$. Jene Diskriminante ist aber (Kap. 1, Formel (82)) gleich dem

Produkte aus der e^{ten} Potenz der Diskriminante der Gleichung (20), der ϱ_1 genügt, ein Ausdruck, der wegen der Irreduktibilität dieser Gleichung (mod. p) relativ prim ist gegen p, und der für den Körper $K(\varrho_1)$ gebildeten Norm der bezüglichen Relativdiskriminante von π_{11}. Dieser letzteren ist mithin die Grundzahl des Abbildungskörpers, was ihre Teilbarkeit durch p betrifft, äquivalent. Die gedachte Relativdiskriminante ist aber das Produkt

$$\Pi(\pi_{1\alpha} - \pi_{1\beta}), \quad (\alpha \gtrless \beta = 1, 2, \cdots, e)$$

demnach jene Norm gleich

$$\Pi\, \Psi_k'(\pi_{kh}) \quad \begin{pmatrix} k = 1, 2, \cdots, f \\ h = 1, 2, \cdots, e \end{pmatrix} \tag{36}$$

d. i. gleich der in bezug auf den Abbildungskörper $K(\pi_{11};\, \varrho_1)$ gebildeten Norm des Ausdrucks $\Psi_1'(\pi_{11})$.

Hier bemerke man nun, daß die Gesamtheit derjenigen Zahlen des Abbildungskörpers $K(\pi_{11};\, \varrho_1)$, welche den Zahlen eines Ideals in $K(\omega)$ entsprechen, ein Ideal jenes Körpers ist, wie auch umgekehrt. Denn, ist α eine Zahl jenes Ideals und α_1 die ihr entsprechende Zahl des Abbildungskörpers, ζ_1 aber irgend eine ganze Zahl des letztern und ζ die ihr entsprechende ebenfalls ganze Zahl in $K(\omega)$, so ist $\zeta\alpha$ eine Zahl des Ideals in $K(\omega)$ und deshalb die ihr entsprechende Zahl $\zeta_1\alpha_1$ eine Zahl der gedachten Gesamtheit, wodurch diese sich als ein Ideal charakterisiert. Man übersieht leicht, daß beide einander entsprechende Ideale gleichzeitig Primideale, insbesondere gleichzeitig Primteiler von p sind und daß, wenn jenes die Zahl π, so dieses die Zahl π_{11} enthält und umgekehrt. Hieraus ergibt sich dann, daß es im Abbildungskörper einen einzigen Primteiler $\mathfrak{p}$ von p gibt, der in π_{11} und zwar genau einmal aufgeht. Man darf daher in Kroneckerscher Weise sagen, $\mathfrak{p}$ sei äquivalent mit $pz + \pi_{11}u$, in Zeichen:

$$\mathfrak{p} \sim pz + \pi_{11}u,$$

und erschließt nun aus der Gleichung (30), der π_{11} genügt, daß p mit $\mathfrak{p}^e$ oder $\mathfrak{p}$ mit $p^{\frac{1}{e}}$ äquivalent ist, sowie die in bezug

auf den Abbildungskörper vom Grade ef genommene Norm von $\bar{\mathfrak{p}}$ mit p^f äquivalent sein muß:

$$N(\bar{\mathfrak{p}}) \sim p^f.$$

Man erinnere sich ferner, daß im Ausdrucke

$$\Psi'(\pi) = e\pi^{e-1} + pC_{e-1}(e-1)\pi^{e-2} + \cdots + pC_1$$

jeder der einzelnen Summanden in bezug auf $\mathfrak{p}$ von verschiedener Ordnung, die Ordnung des gesamten Ausdrucks also diejenige seines niedrigsten Gliedes ist. Gleicherweise wird die Ordnung von $\Psi_1'(\pi_{11})$ in bezug auf $\bar{\mathfrak{p}}$ diejenige seines niedrigsten Gliedes sein, und wenn sie durch die Potenz $\bar{\mathfrak{p}}^{v-1}$ bezeichnet wird, so wird der ganze Ausdruck $\Psi_1'(\pi_{11})$ mit der gebrochenen Potenz $p^{\frac{v-1}{e}}$ äquivalent sein und gleiches gelten von jedem der konjugierten Faktoren des Produkts (36). Demnach wird dies gesamte Produkt äquivalent sein mit

$$\left(p^{\frac{v-1}{e}}\right)^{ef} = p^{(v-1)f}.$$

Die Zahl v möge im Anschluß an die Betrachtungen der Nr. 2 die Verzweigungszahl heißen, ebenso wie die Grundzahl oder Diskriminante des Abbildungskörpers die bezügliche Verzweigungsdiskriminante.

Im regulären Falle ist

$$v = e, \tag{37}$$

denn dann ist

$$\Psi(x) = x^e + pB_0 \tag{38}$$

also $\Psi_1'(\pi_{11}) = e\pi_{11}^{e-1}$, mithin, da e durch p nicht teilbar ist, von der Ordnung $e-1$, also e die Verzweigungszahl. Im singulären Falle aber ist $\Psi(x)$ von der allgemeineren Form (17) also, wenn $e = pC_e$ gesetzt wird,

$$\Psi_1'(\pi_{11}) = pC_e\pi_{11}^{e-1} + pC_{e-1}(e-1)\pi_{11}^{e-2} + \cdots$$
$$+ pC_i \cdot i\pi_{11}^{i-1} + \cdots + pC_1.$$

Ist dann etwa piC_i derjenige Koeffizient, welcher erstens die niedrigste Potenz p^{ε_i} von p enthält und für den zweitens der Exponent i am kleinsten ist, so wird $\Psi_1'(\pi_{11})$ die Ordnung $e\varepsilon_i + i - 1$ des Gliedes

$$pC_i \cdot i\pi_{11}^{i-1}$$

besitzen und daher die Verzweigungszahl

$$v = e\varepsilon_i + i \tag{37a}$$

sein. Man erhält also das Resultat:

Ist $\mathfrak{p}$ ein Primidealfaktor f^{ten} Grades von p im Körper $K(\omega)$, der genau e Mal in p aufgeht, und $K(\pi_{11};\ \varrho_1)$ der zugehörige Abbildungskörper, so ist die Diskriminante des letztern genau durch die Potenz $p^{(v-1)f}$ teilbar, wo v die Verzweigungszahl bedeutet, welche durch die Formel (37) bezw. (37a) bestimmt wird.

Den kleinsten Wert hat die Verzweigungszahl im regulären Falle, nämlich $v = e$; im singulären Falle aber ist, selbst wenn $\Psi(x)$ die einfache Gestalt (38) hat, v größer als e, da dann ε_i sowohl wie i mindestens gleich 1 ist, und in ihm erreicht v den größten Wert offenbar dann, wenn

$$e\pi_{11}^{e-1}$$

das Glied niedrigster Ordnung in $\Psi_1{}'(\pi_{11})$ ist, und wird alsdann, wenn e genau durch p^ε aufgeht, $v = (\varepsilon + 1)e$. Schon Dedekind sprach dieses Resultat als eine Vermutung aus am Schlusse seiner Abhandlung „Über die Diskriminanten endlicher Körper“ in Götting. Abh. 29, 1882.

5. Nachdem dies festgestellt worden ist, bezeichnen wir mit

$$\omega_1,\ \omega_2,\ \cdots,\ \omega_n \tag{39}$$

die ganze Zahl ω mit ihren Konjugierten und ebenso mit

$$K(\omega_1),\ K(\omega_2),\ \cdots,\ K(\omega_n) \tag{40}$$

den Körper $K(\omega)$ mit seinen Konjugierten. Ist dann K der aus den sämtlichen Konjugierten (40) gebildete Galoissche Körper und P ein beliebiger Primidealfaktor von p in K, so ist unter den Primidealfaktoren, in welche p in jedem der konjugierten Körper (40) zerfällt, je ein bestimmter $\mathfrak{p}', \mathfrak{p}'', \cdots, \mathfrak{p}^{(n)}$ durch P teilbar; in bezug auf jeden dieser Primteiler läßt sich die Betrachtung der Nr. 1 wiederholen, nämlich zwei den Zahlen ϱ, π entsprechende Entwicklungszahlen $\varrho^{(i)}$, $\pi^{(i)}$ als Wurzeln zweier mit (15) und (16) analogen Kongruenzen

$$P^{(i)}(x) \equiv 0, \quad \Psi^{(i)}(x) \equiv 0 \pmod{\mathfrak{p}^{(i)m}}$$

und aus den Wurzeln der mit (20) und (22) analogen Gleichungen

(41) $$P^{(i)}(x) = 0, \quad \Psi_k^{(i)}(x) = 0$$

ein Körper $K(\pi_{11}^{(i)}; \varrho_1^{(i)})$ mit seinen Konjugierten bestimmen. Denkt man dies für jeden der Primidealfaktoren P von p in K ausgeführt und versteht nunmehr unter dem Körper $\mathfrak{K}$ der vorigen Nummer einen Galoisschen Körper, welcher nicht nur den Körper K, sondern alle auf die eben bezeichnete Weise gebildeten Körper $K(\pi_{11}^{(i)}; \varrho_1^{(i)})$ mit ihren Konjugierten in sich enthält, und unter dem Primideale $\mathfrak{P}$ irgend einen Primidealfaktor der Ideale P, d. h. einen beliebigen Primidealfaktor von p in $\mathfrak{K}$, so gilt offenbar die Betrachtung der vorigen Nummern in bezug auf dieses Primideal $\mathfrak{P}$ für jeden der konjugierten Körper (40) und es ist also für jeden Körper $K(\omega_i)$ ein bestimmter anderer Körper $K(\pi_{11}^{(i)}; \varrho_1^{(i)})$ angebbar, auf welchen jener (mod. $\mathfrak{P}^m$) abgebildet werden kann und umgekehrt, indem sich eine Zahl $\omega_i^{(0)}$ dieses Körpers von der Gestalt

(42) $$\omega_i^{(0)} = A_{r_i}^{(i)} \pi_{11}^{(i) r_i} + A_{r_i+1}^{(i)} \pi_{11}^{(i) r_i+1} + \cdots$$

angeben läßt, für welche

(43) $$\omega_i \equiv \omega_i^{(0)} \pmod{\mathfrak{P}^m}$$

ist. So erhält man für die n konjugierten Körper

$$K(\omega_1), \; K(\omega_2), \; \cdots, \; K(\omega_n)$$

ebensoviel Abbildungskörper

(44) $$K(\pi'_{11}; \varrho'_1), \; K(\pi''_{11}; \varrho''_1), \; \cdots, \; K(\pi_{11}^{(n)}; \varrho_1^{(n)})$$

(mod. $\mathfrak{P}^m$).

Dies vorausgeschickt sei

(45) $$F(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_n)$$

die ganzzahlige Gleichung, der die Zahlen (39) genügen. Wegen (43) findet sich

$$F(x) \equiv (x - \omega_1^{(0)})(x - \omega_2^{(0)}) \cdots (x - \omega_n^{(0)}) \pmod{\mathfrak{P}^m}$$

und daher

$$F(\omega_i^{(0)}) \equiv 0 \pmod{\mathfrak{P}^m},$$

d. h. jede der Zahlen (42) ist eine Wurzel der Kongruenz

(46) $$F(x) \equiv 0 \pmod{\mathfrak{P}^m};$$

aber auch jede solche Wurzel muß nach beliebig hoher Potenz von $\mathfrak{P}$ einer jener Zahlen kongruent sein. Zudem sind diese (mod. $\mathfrak{P}^m$) inkongruent, da sonst die Diskriminante der

Funktion $F(x)$ durch die beliebig hohe Potenz $\mathfrak{P}^m$ oder — als rationale ganze Zahl — durch jede noch so hohe Potenz von p teilbar, also Null sein müßte, während doch die Gleichung $F(x) = 0$ irreduktibel ist. Diese n Wurzeln (42) lassen sich aber auch als Wurzeln der Kongruenz

$$F(x) \equiv 0 \tag{47}$$

nach einer beliebig hohen Potenz von p als Modulus charakterisieren. Entwickelt man nämlich den Ausdruck

$$F(\omega_i^{(0)})$$

nach Potenzen von $\varrho_1^{(i)}$ und $\pi_{11}^{(i)}$, so nimmt die Kongruenz $F(\omega_i^{(0)}) \equiv 0 \pmod{\mathfrak{P}^m}$, reduziert durch die Gleichungen (41) von den Graden $e^{(i)}$, $f^{(i)}$ resp., denen jene Größen genügen, die Gestalt an:

$$\sum_{g=0}^{f^{(i)}-1} \sum_{h=0}^{e^{(i)}-1} a_{gh} \cdot \varrho_1^{(i)g} \cdot \pi_{11}^{(i)h} \equiv 0 \pmod{\mathfrak{P}^m},$$

welche nach Nr. 3 nur identisch bestehen kann, wenn nämlich jedes einzelne Glied

$$a_{gh} \cdot \varrho_1^{(i)g} \cdot \pi_{11}^{(i)h}$$

der Summe für sich durch $\mathfrak{P}^m$ teilbar ist; für einen hinreichend großen Wert von m müßte also jeder der Koeffizienten a_{gh} durch eine beliebig hohe Potenz von $\mathfrak{P}$ und somit auch von p teilbar, d. h. die Kongruenz (47) in bezug auf diese Potenz von p als Modulus durch die Zahl $\omega_i^{(0)}$ erfüllt sein.

Leistet aber $\omega_i^{(0)}$ der Kongruenz (mod. p^m) Genüge, so gilt dasselbe von allen $e^{(i)}f^{(i)}$ zu $\omega_i^{(0)}$ in bezug auf den Abbildungskörper $K(\pi_{11}^{(i)}; \varrho_1^{(i)})$ vom Grade $e^{(i)}f^{(i)}$, dem $\omega_i^{(0)}$ angehört, konjugierten Zahlen; diese $e^{(i)}f^{(i)}$ konjugierten Zahlen sind demnach auch sämtlich Wurzeln der Kongruenz (46) für den entsprechenden Modulus $\mathfrak{P}^m$, und zwar verschiedene solche Wurzeln, da, wenn zwei von ihnen (mod. $\mathfrak{P}^m$) kongruent wären, die Diskriminante jener Zahlen, nämlich die Diskriminante der irreduktibeln Gleichung vom Grade $e^{(i)}f^{(i)}$, der nach Nr. 3 die Zahl $\omega_i^{(0)}$ dieses Grades genügt, durch $\mathfrak{P}^m$ oder, als rationale ganze Zahl, durch jede noch so hohe Potenz von p teilbar also Null sein müßte, was nicht sein kann. Man ersieht hieraus, daß unter den Zahlen (42) sich $e^{(i)}f^{(i)}$ Zahlen

befinden, welche jenen in bezug auf den Abbildungskörper konjugierten Zahlen kongruent sind und deshalb durch sie ersetzt werden dürfen; und da diese Betrachtung für jeden Wert des Index i zulässig ist, so erschließt man folgenden Satz:

Die n Abbildungskörper (44) zerfallen in eine Anzahl Systeme von Körpern, deren jedes aus einer geringeren Anzahl unter sich konjugierter Körper gebildet ist.

Wenn die Primzahl p, was wir, um die Begriffe zu fixieren, hinfort voraussetzen wollen, im Körper $K(\omega)$ aus drei verschiedenen Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ von den Graden f_1, f_2, f_3 zusammengesetzt ist:

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3},$$

so gibt es drei Systeme von resp.

$$\nu_1 = e_1 f_1, \quad \nu_2 = e_2 f_2, \quad \nu_3 = e_3 f_3$$

unter einander konjugierten Körpern

$$K(\gamma_1),\ K(\gamma_2), \cdots, K(\gamma_{\nu_1});\ K(\delta_1), \cdots, K(\delta_{\nu_2});\ K(\varepsilon_1), \cdots, K(\varepsilon_{\nu_3}),$$

auf welche die n Körper $K(\omega_1)$, $K(\omega_2)$, $\cdots$, $K(\omega_n)$ (mod. $\mathfrak{P}^m$) abgebildet sind.

6. Bezeichnen nun $\zeta_1, \zeta_2, \cdots, \zeta_n$ irgend eine ganze Zahl des Körpers $K(\omega_1)$ mit ihren Konjugierten, so ist ζ_1 einer Zahl des Abbildungskörpers $K(\gamma_1) = K(\pi'_{11};\ \varrho_1')$ nach dem Modulus $\mathfrak{P}^m$ kongruent und es besteht analog mit (14) eine Kongruenz, welche, auf den kleinsten Grad reduziert, die Gestalt

$$\zeta_1 \equiv \sum_{g=0}^{f_1-1}\sum_{h=0}^{e_1-1} a_{gh}\varrho_1'^{g}\pi_{11}'^{h} \pmod{\mathfrak{P}^m}$$

oder einfacher, wenn die $\nu_1 = e_1 f_1$ Zahlen $\varrho_1'^{g}\pi_{11}'^{h}$ in beliebiger aber fester Reihenfolge durch

$$(48) \qquad \gamma_1^{(1)},\ \gamma_1^{(2)}, \cdots, \gamma_1^{(\nu_1)}$$

bezeichnet werden, die Gestalt

$$\zeta_1 \equiv a_1\gamma_1^{(1)} + a_2\gamma_1^{(2)} + \cdots + a_{\nu_1}\gamma_1^{(\nu_1)} \pmod{\mathfrak{P}^m}$$

erhält. Bedeuten

$$\gamma_i^{(1)},\ \gamma_i^{(2)}, \cdots, \gamma_i^{(\nu_1)}$$

die dem Körper $K(\gamma_i)$ angehörigen Konjugierten der Zahlen (48),

so findet sich für die dem Körper $K(\omega_i)$ angehörige Konjugierte ζ_i von ζ_1 die entsprechende Kongruenz

$$(48^a) \qquad \zeta_i \equiv a_1 \gamma_i^{(1)} + a_2 \gamma_i^{(2)} + \cdots + a_{\nu_1} \gamma_i^{(\nu_1)} \pmod{\mathfrak{P}^m} \quad (i = 1, 2, \cdots, \nu_1)$$

und man findet bei analoger Bedeutung der Zeichen $\delta_1^{(1)}, \delta_1^{(2)}, \cdots, \delta_1^{(\nu_2)}; \varepsilon_1^{(1)}, \varepsilon_1^{(2)}, \cdots, \varepsilon_1^{(\nu_3)}$ für die übrigen Konjugierten von ζ_1 die ferneren Kongruenzen:

$$(48^b) \qquad \zeta_{\nu_1+h} \equiv b_1 \delta_h^{(1)} + b_2 \delta_h^{(2)} + \cdots + b_{\nu_2} \delta_h^{(\nu_2)} \quad (h = 1, 2, \cdots, \nu_2)$$

$$(48^c) \qquad \zeta_{\nu_1+\nu_2+k} \equiv c_1 \varepsilon_k^{(1)} + c_2 \varepsilon_k^{(2)} + \cdots + c_{\nu_3} \varepsilon_k^{(\nu_3)}. \quad (k = 1, 2, \cdots, \nu_3)$$

Nunmehr bedeute

$$(49) \qquad \zeta_1^{(1)}, \zeta_1^{(2)}, \cdots, \zeta_1^{(n)}$$

irgend ein unabhängiges System von n Zahlen des Körpers $K(\omega_1)$; stellt man es mit den zu ihm konjugierten Systemen zu einer Matrix zusammen:

$$(50) \qquad \left\| \begin{matrix} \zeta_1^{(1)}, & \zeta_1^{(2)}, & \cdots, & \zeta_1^{(n)} \\ \zeta_2^{(1)}, & \zeta_2^{(2)}, & \cdots, & \zeta_2^{(n)} \\ \cdot & \cdot & \cdot & \cdot \\ \zeta_n^{(1)}, & \zeta_n^{(2)}, & \cdots, & \zeta_n^{(n)} \end{matrix} \right\|$$

und bildet für jede der Zahlen (49) die entsprechenden Kongruenzen ($48^{a,b,c}$), so werden in jeder Kolonne der Matrix die ν_1 ersten Elemente (mod. $\mathfrak{P}^m$) durch lineare Funktionen der Zahlen $\gamma_1^{(1)}, \gamma_1^{(2)}, \cdots, \gamma_1^{(\nu_1)}$ resp. ihrer Konjugierten, die ν_2 folgenden durch lineare Funktionen der $\delta_1^{(1)}, \delta_1^{(2)}, \cdots, \delta_1^{(\nu_2)}$ resp. ihrer Konjugierten usw. ersetzt werden können. Die Betrachtung der höchsten Potenzen von $\mathfrak{P}$, welche dann allen Elementen einer Kolonne gemeinsam sind, verstattet durch eine Reihe einfacher Umformungen zu zeigen (s. darüber § 7 u. 8 der Henselschen Arbeit), daß aus dem Systeme (49) ein anderes System

$$(51) \qquad \xi_1^{(1)}, \xi_1^{(2)}, \cdots, \xi_1^{(n)}$$

von n unabhängigen Zahlen hergeleitet werden kann von der besonderen Beschaffenheit, daß die Matrix seiner Elemente und deren Konjugierten der folgenden „zerfallenden" Matrix (mod. $\mathfrak{P}^m$) kongruent ist:

$$(52)\qquad \begin{Vmatrix} \gamma_1^{(1)}, & \cdots & \gamma_1^{(\nu_1)}, & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \gamma_{\nu_1}^{(1)} & \cdots & \gamma_{\nu_1}^{(\nu_1)} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \delta_1^{(1)} & \cdots & \delta_1^{(\nu_2)} & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdots & 0 & \delta_{\nu_2}^{(1)} & \cdots & \delta_{\nu_2}^{(\nu_2)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \varepsilon_1^{(1)} & \cdots & \varepsilon_1^{(\nu_3)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \varepsilon_{\nu_3}^{(1)} & \cdots & \varepsilon_{\nu_3}^{(\nu_3)} \end{Vmatrix}.$$

Man sieht leicht ein, daß letzteres System ein Fundamentalsystem (mod. p) sein muß. Denn bestände eine Kongruenz

$$u_1 \xi_1^{(1)} + u_2 \xi_1^{(2)} + \cdots + u_n \xi_1^{(n)} \equiv 0 \pmod{p}$$

mit ganzzahligen Koeffizienten, so müßte dieser Ausdruck nebst seinen sämtlichen Konjugierten durch die gleiche Potenz des Galoisschen Primteilers $\mathfrak{P}$ aufgehen, durch welche p teilbar ist, und somit würden, wenn $\mathfrak{P}^\mu$ diese Potenz ist, aus der Kongruenz der Matrix jenes Systems mit der Matrix (52) nach beliebig hoher Potenz von $\mathfrak{P}$ die folgenden Kongruenzen:

$$\left.\begin{array}{c} u_1 \gamma_i^{(1)} + \cdots + u_{\nu_1} \gamma_i^{(\nu_1)} \equiv 0 \\ (i = 1, 2, \cdots, \nu_1) \\ u_{\nu_1+1} \delta_h^{(1)} + \cdots + u_{\nu_1+\nu_2} \delta_h^{(\nu_2)} \equiv 0 \\ (h = 1, 2, \cdots, \nu_2) \\ u_{\nu_1+\nu_2+1} \varepsilon_k^{(1)} + \cdots + u_{\nu_1+\nu_2+\nu_3} \varepsilon_k^{(\nu_3)} \equiv 0 \\ (k = 1, 2, \cdots, \nu_3) \end{array}\right\} \pmod{\mathfrak{P}^\mu}$$

hervorgehen, von denen das erste (nach Nr. 3) nur bestehen kann, wenn sämtliche $u_1, u_2, \cdots, u_{\nu_1}$ durch p teilbar sind, während aus den übrigen aus gleichen Gründen die Teilbarkeit aller folgenden u_i durch p sich ergibt.

Mit Rücksicht hierauf ist die Diskriminante des Systems (51), was ihre Teilbarkeit durch p anbelangt, der Diskriminante D des Körpers $K(\omega_1)$ äquivalent. Andererseits ist sie in bezug auf den Modulus $\mathfrak{P}^m$ dem Quadrate der aus den Elementen der Matrix (52) gebildeten Determinante kongruent, also kongruent dem Produkte

$$(53)\qquad \Gamma^2 \cdot \Delta^2 \cdot E^2,$$

in welchem Γ^2, Δ^2, E^2 die Diskriminanten der Systeme $\gamma_k^{(i)}$, $\delta_k^{(i)}$, $\varepsilon_k^{(i)}$ resp., d. h. den verschiedenen Verzweigungsdiskrimi-

nanten mit bezug auf die Primzahl p äquivalent sind. Nun ist $\mathfrak{P}$ ein beliebiger Primidealfaktor von p im Körper $\mathfrak{K}$; dem Gesagten zufolge muß er in der Diskriminante D genau ebenso oft aufgehen, wie in dem Produkte (53), und somit erhalten wir den folgenden eleganten *Hensel*schen Satz:

Jeder Primteiler $\mathfrak{P}$ von p im Körper $\mathfrak{K}$ und somit auch die Primzahl p selbst geht in der Diskriminante D des Körpers $K(\omega)$ genau so oft auf, wie im Produkte der für diesen Körper und die Primzahl p vorhandenen Verzweigungsdiskriminanten.

Die Schlußsätze der Nr. 4 gestatten hiernach, für die Potenz von p, durch welche D teilbar ist, den genauen Ausdruck aufzustellen. Bezeichnen nämlich, wenn wieder der Bestimmtheit wegen

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3}$$

vorausgesetzt wird, wo $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ die verschiedenen Primidealfaktoren von p im Körper $K(\omega)$ bedeuten, f_1, f_2, f_3 die Grade der letzteren und v_1, v_2, v_3 die ihnen entsprechenden, nach Nr. 4 zu bestimmenden Verzweigungszahlen, so ist D genau teilbar durch die Potenz

$$p^{(v_1-1)f_1+(v_2-1)f_2+(v_3-1)f_3}$$

mit dem Exponenten

$$d = (v_1 - 1)f_1 + (v_2 - 1)f_2 + (v_3 - 1)f_3. \tag{54}$$

Da der letztere im regulären Falle gleich

$$(e_1 - 1)f_1 + (e_2 - 1)f_2 + (e_3 - 1)f_3,$$

andernfalls aber, d. h. für die singulären Primzahlen p, bei denen einer der Exponenten e_i durch p teilbar ist, größer ist als dieser Wert, so sieht man den in Kap. 7, Nr. 13 gewonnenen Satz über die Zusammensetzung der Grundzahl bestätigt. Während aber durch diesen Satz nur eine Minimalgrenze für die Häufigkeit der einzelnen Primfaktoren in der Zerlegung der Grundzahl bestimmt wurde, liefert jetzt die für den Exponenten d gegebene Formel (54) das Gesetz, nach welchem die völlig genaue Zusammensetzung der Grundzahl aus ihren Primfaktoren zu ermitteln ist.

Bemerkungen.

Zu Seite 1. R. Dedekind und andere Forscher haben Definitionen des Irrationellen aufgestellt, denen der Grenzbegriff fern bleibt; für den Zweck der einleitenden Zeilen schien es nicht erforderlich, auf solche prinzipiellen Gesichtspunkte einzugehen.

Zu Kapitel 3, Nr. 1. Auf Grund des Gaußschen Fundamentalsatzes (Kap. 1, Nr. 1), nach welchem die Primfunktionen in der Zerlegung (13) nichts anderes als die Linearfaktoren $x - \alpha$ sind, welche den Wurzeln α der Gleichung $F(x) = 0$ entsprechen, konnte diese Nummer sehr viel einfacher gestaltet werden; doch ist eine solche Form der Darstellung gewählt worden, daß sie sogleich auch für den Bereich der ganzen Funktionen, deren Koeffizienten rational (oder einem gegebenen Rationalitätsbereiche angehörig) sind, bestehen bleibt.

Zu Seite 96. Die Formel (50) gilt auch für $p = 2$, da alsdann $+1$ und -1 kongruent sind.

Zu Kapitel 4, Nr. 4. Zur Herleitung des Hauptsatzes S. 128 ist es nicht erforderlich, die Zahlen (24) mit ganzzahligen Koeffizienten zu wählen; es genügt, daß es im Ideale n unabhängige Zahlen gibt; dies sind z. B. jedenfalls die Zahlen

$$\theta_1 = N(\theta) \cdot \gamma_1, \cdots, \theta_n = N(\theta) \cdot \gamma_n,$$

wenn θ eine von Null verschiedene Zahl des Ideales ist. Jene Wahl geschah vielmehr aus anderer Rücksicht. Man kann, ausgehend von (23) statt von (25), mittels völlig entsprechender Betrachtungen unmittelbar die Existenz einer Basis für die Gesamtheit $\mathfrak{g}$ nachweisen. Bilden aber $\gamma_1, \gamma_2, \cdots, \gamma_n$ eine solche, und werden nun die Zahlen $\theta_1, \theta_2, \cdots, \theta_n$, wie es bei (24) geschehen ist, und noch spezieller jede Zahl θ_s unter den Zahlen

$$g_1^{(s)} \cdot \gamma_1 + g_2^{(s)} \cdot \gamma_2 + \cdots + g_s^{(s)} \cdot \gamma_s$$

des Ideales $\mathfrak{j}$ so gewählt, daß der Koeffizient $g_s^{(s)}$ den kleinsten positiven ganzzahligen Wert erhält, so bilden $\theta_1, \theta_2, \cdots, \theta_n$ sogleich eine Basis des Ideals $\mathfrak{j}$, man hat

$$\mathfrak{j} = [\theta_1, \theta_2, \cdots, \theta_n]$$

und nach (46) und (47)

$$\mathfrak{N}(\mathfrak{j}) = g_1^{(1)} \cdot g_2^{(2)} \cdots g_n^{(n)}.$$

Denn, da jede Zahl θ des Ideales in die Form

$$\theta = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_n\gamma_n$$

mit ganzzahligen c_i gesetzt werden kann, erhält man durch passende Bestimmung der ganzen Zahlen $h_1, h_2, \cdots, h_n$ die Beziehung

$$\theta = h_1\theta_1 + h_2\theta_2 + \cdots + h_n\theta_n + \theta',$$

wo in der im Ideale enthaltenen Zahl

$$\theta' = c_1'\gamma_1 + c_2'\gamma_2 + \cdots + c_n'\gamma_n$$

die Koeffizienten c_i' den Bedingungen

$$0 \overline{\lessgtr} c_s' < g_s^{(s)}$$
$$(s = 1, 2, \cdots, n)$$

gehorchen, was nach der Bedeutung der Zahlen $g_s^{(s)}$ nicht anders sein kann, als wenn $c_s' = 0$ (für $s = 1, 2, \cdots, n$), also auch $\theta' = 0$ und

$$\theta = h_1\theta_1 + h_2\theta_2 + \cdots + h_n\theta_n$$

ist. —

Zu Seite 153, Anmerkung s. Journ. de Math. 3. sér. t. 6.

Zu Seite 173. Die Zahlen β_i sind rationale symmetrische Funktionen der zur Erzeugenden des Körpers konjugierten Zahlen, mithin rationale Funktionen der Erzeugenden selbst, d. h. sie sind Zahlen des Körpers, zudem aber, als algebraisch ganz, Zahlen in $\mathfrak{g}$. Die γ_i sind rationale symmetrische Funktionen der Erzeugenden und ihrer Konjugierten, also dem Rationalitätsbereiche des Körpers angehörige Zahlen und zudem, als algebraisch ganz, rationale ganze Zahlen.

Zu Seite 243. Der Satz (Formel (151)) leuchtet für den Fall, daß ϱ eine Primitivzahl ist, unmittelbar daraus ein, daß γ einer Potenz von ϱ, welche mittels $P(\varrho) \equiv 0 \pmod{\mathfrak{p}}$ auf die Form (151) gebracht werden kann, kongruent ist.

Seite 286, Z. 3 lies Nr. 7 statt Nr. 6.

Zu Seite 336, Z. 2. Gemeint ist hier Minkowskis Darstellung der Theorie der Einheiten (in seiner Geometrie der Zahlen § 44), welche in Hilberts Bericht über algebraische Zahlkörper im wesentlichen reproduziert ist.

Zu Seite 344. Der hier gegebene Beweis des zweiten Diskriminantensatzes weist, wie — scheint mir — auch der Hilbertsche, dem wir zumeist gefolgt sind, eine Lücke, indem nicht ersichtlich wird, daß die Zahl $w^{(r+1)}$ auch von der konjugiert imaginären Zahl $w^{(r+\varrho+1)}$ verschieden, nämlich nicht reell ist. Es sei daher für diesen Satz hier noch auf Hermites an Borchardt

gerichteten Brief (Journ. f. Math. 53, 1857, p. 182) verwiesen. Übrigens läßt sich von dem Satze aus auf Grund einer von Minkowski gegebenen unteren Grenze für die Grundzahl eines Körpers einsehen, daß nicht nur für einen gegebenen Grad n, sondern auch überhaupt die Anzahl der Körper mit gegebener Grundzahl eine nur endliche ist; s. Minkowskis Geom. d. Zahlen § 42.

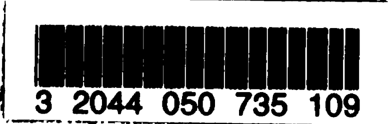
Seite 358, Z. 7 ergänze 11 als Nummer des neu beginnenden Artikels.

Zu Seite 362. Die letzten vier Zeilen enthalten ein kleines Versehen; es muß heißen: Seine Basiszahlen $\lambda_1, \lambda_2, \cdots, \lambda_n$ lassen sich durch die dortigen Formeln (53) darstellen, in denen allgemein $\mu_i' = \omega_i$ zu denken ist; sie nehmen daher — oder einfacher, weil sie Zahlen in $\mathfrak{o}$ sind — die Gestalt (4) an, deren Koeffizienten usw.

Zu Seite 460. Die Ausdrücke (47) stellen zwar nicht Zahlen, sondern Ideale dar, doch darf man dafür bei den nachfolgenden Betrachtungen Zahlen setzen, die resp. in ihnen enthalten sind.

Seite 522, Z. 10 lies „erzeugende ganze Zahl ω".

Seite 525, Z. 3 streiche (mod. p).


3 2044 050 735 109
